

JoeSandbox Cloud BASIC



ID: 413047

Sample Name:

4e021da2_by_Libranalysis.dll

Cookbook: default.jbs

Time: 07:04:51

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 4e021da2_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
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
Contacted IPs	8
Public	8
General Information	8
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	10
ASN	11
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	13
General	13
File Icon	14
Static PE Info	14
General	14
Entrypoint Preview	14
Rich Headers	15
Data Directories	15
Sections	15
Resources	16
Imports	16
Version Infos	16
Network Behavior	16
UDP Packets	16

DNS Answers	18
Code Manipulations	18
Statistics	18
Behavior	18
System Behavior	18
Analysis Process: loadll32.exe PID: 5608 Parent PID: 5748	18
General	18
File Activities	19
Analysis Process: cmd.exe PID: 5420 Parent PID: 5608	19
General	19
File Activities	19
Analysis Process: rundll32.exe PID: 5508 Parent PID: 5420	19
General	19
Analysis Process: WerFault.exe PID: 2308 Parent PID: 5508	19
General	19
File Activities	20
File Created	20
File Deleted	20
File Written	20
Registry Activities	41
Key Created	41
Key Value Created	41
Disassembly	42
Code Analysis	42

Analysis Report 4e021da2_by_Libranalysis.dll

Overview

General Information

Sample Name:

4e021da2_by_Libranalysis.dll

Analysis ID:

413047

MD5:

4e021da22c2701..

SHA1:

e791b7c6b5b3a9..

SHA256:

e39faf4e4460a28..

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Dridex

Score:

72

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected Dridex unpacked file

C2 URLs / IPs found in malware con...

Machine Learning detection for samp...

Checks if the current process is bein...

Contains functionality to check if a d...

Contains functionality to query locale...

Creates a process in suspended mo...

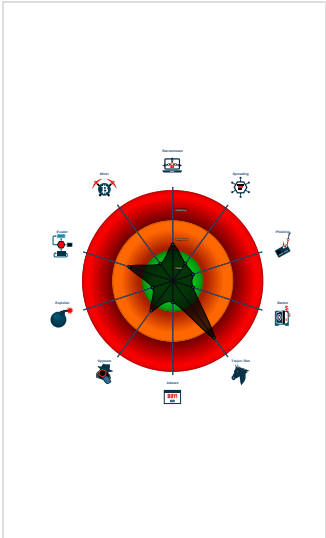
Detected potential crypto function

IP address seen in connection with o...

Internet Provider seen in connection...

One or more processes crash

Classification



Startup

■ System is w10x64

loadll32.exe (PID: 5608 cmdline: loadll32.exe 'C:\Users\user\Desktop\4e021da2_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 5420 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\4e021da2_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 5508 cmdline: rundll32.exe 'C:\Users\user\Desktop\4e021da2_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 2308 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5508 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

■ cleanup

Malware Configuration

Threatname: Dridex

```
{
  "Version": 22201,
  "C2 list": [
    "43.229.206.212:443",
    "82.209.17.209:8172",
    "162.241.209.225:4125"
  ],
  "RC4 keys": [
    "16dkGSt0zdHgjuCciXGdSX7UrHkfYSUG8wEUtKNgzHrWMfTGafJbC",
    "39t3NdDhurvp1tFNCpvA5goSylkxjIBtIwHPTv1DPbNEcuIekQC70"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.285424376.0000000010001000.0000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Copyright Joe Security LLC 2021

Page 4 of 42

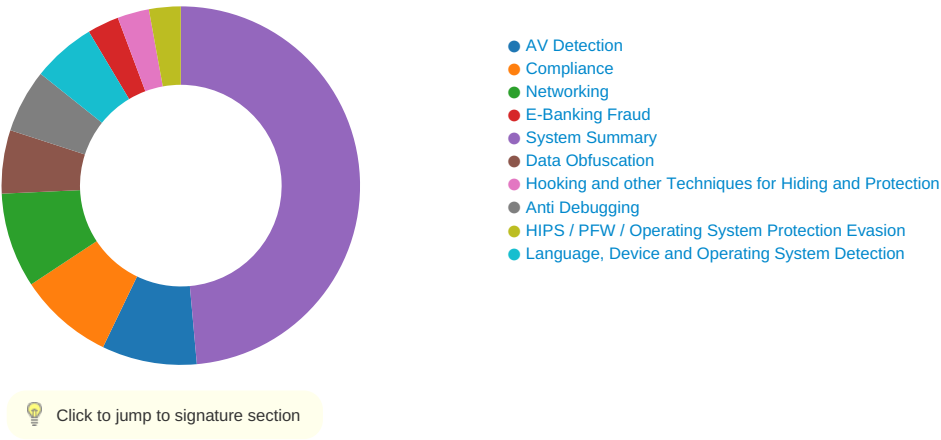
Unpacked PEs

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:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

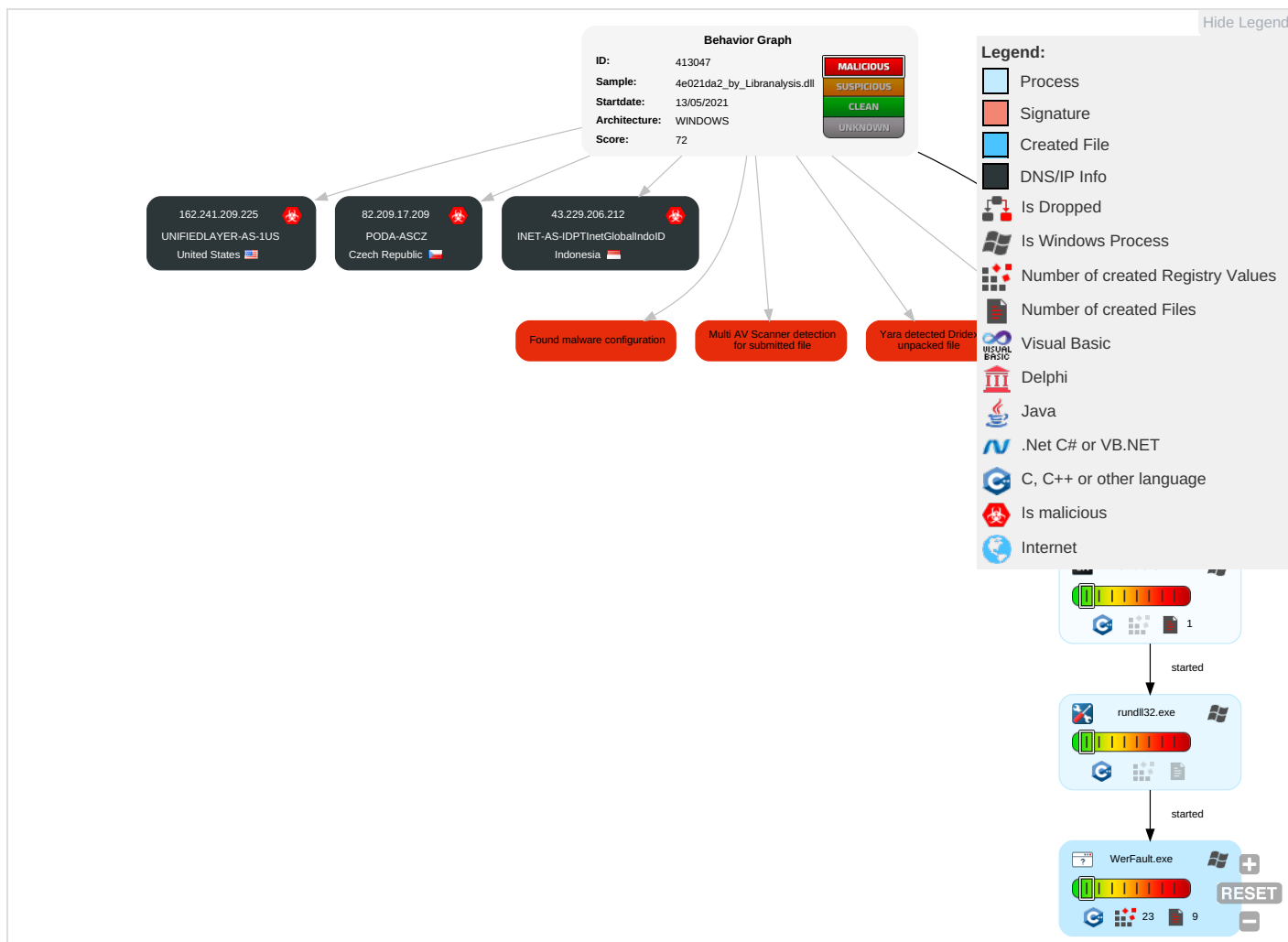
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication

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

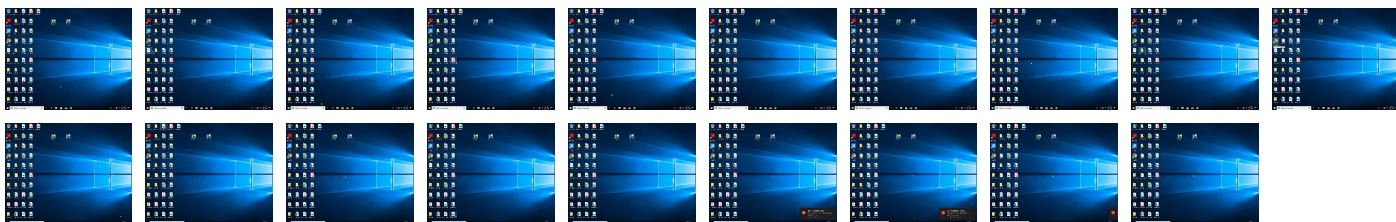
Behavior Graph



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
4e021da2_by_Libranalysis.dll	32%	ReversingLabs	Win32.Trojan.Convagent	
4e021da2_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.35c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
api.globalsign.cloud	0%	Virustotal		Browse

URLs

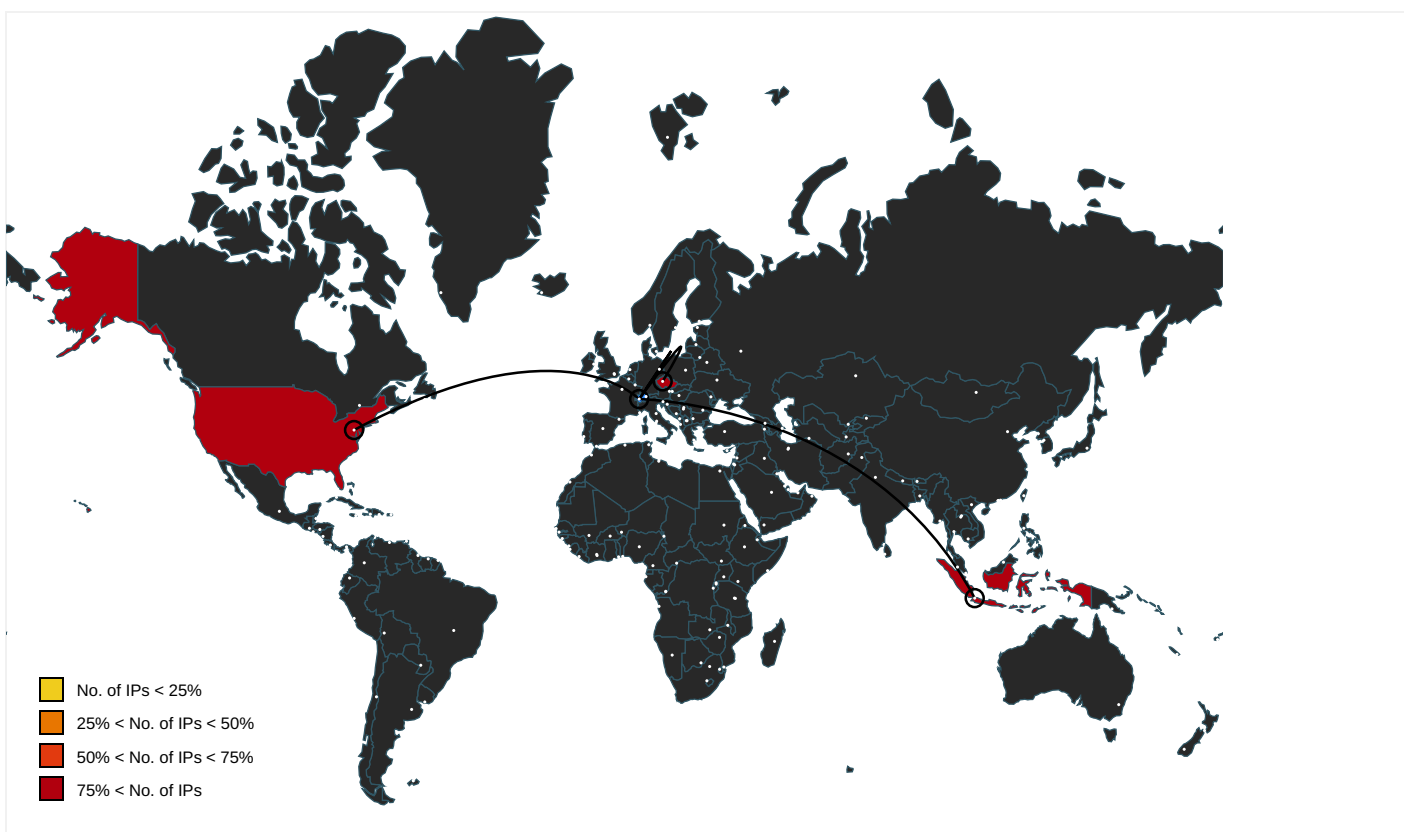
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.globalsign.cloud	104.18.24.243	true	false	0%, Virustotal, Browse	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413047
Start date:	13.05.2021

Start time:	07:04:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4e021da2_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:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 57% (good quality ratio 49.4%) • Quality average: 67.4% • Quality standard deviation: 35.6%
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
82.209.17.209	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.globalsign.cloud	N6hkl66Jq5.dll	Get hash	malicious	Browse	104.18.24.243
	6f61bc36_by_Libranalysis.dll	Get hash	malicious	Browse	104.18.24.243
	Telex.exe	Get hash	malicious	Browse	104.18.24.243
	263a35c3_by_Libranalysis.dll	Get hash	malicious	Browse	104.18.25.243
	POI09876OIUY.exe	Get hash	malicious	Browse	104.18.25.243
	Request Sample products.exe	Get hash	malicious	Browse	104.18.25.243
	6823a552_by_Libranalysis.dll	Get hash	malicious	Browse	104.18.24.243
	3bc8e970_by_Libranalysis.dll	Get hash	malicious	Browse	104.18.25.243
	079c508f_by_Libranalysis.dll	Get hash	malicious	Browse	104.18.25.243
	80df624d_by_Libranalysis.dll	Get hash	malicious	Browse	104.18.24.243
	8333bdd5e1560584a0302e2fe63cf9d81ebe5b48e7e2b.exe	Get hash	malicious	Browse	104.18.24.243
	7b73e459_by_Libranalysis.dll	Get hash	malicious	Browse	104.18.25.243

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IBmH1dux3rkWHAs.exe	Get hash	malicious	Browse	• 104.18.24.243
	INQUIRY.exe	Get hash	malicious	Browse	• 104.18.24.243
	0908000000.exe	Get hash	malicious	Browse	• 104.18.24.243
	urgent request fro quotation CONO GROUP LLC DK9837 46GT.exe	Get hash	malicious	Browse	• 104.18.25.243
	un6IVL1qYU.dll	Get hash	malicious	Browse	• 104.18.25.243
	dVMxk14XPULdIBw.exe	Get hash	malicious	Browse	• 104.18.25.243
	Purchase Order-1245102021.xls	Get hash	malicious	Browse	• 104.18.25.243
	SecuriteInfo.com.Trojan.Win32.Save.a.32673.exe	Get hash	malicious	Browse	• 104.18.25.243

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f8f758f9c9ae6eac81fa9732924e44386348e_82810a17_0958c999\Report	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12480
Entropy (8bit):	3.7664210837651564
Encrypted:	false
SSDEEP:	192:FRG3iy0x5tcHBUXMx4jed+SG/u7ssS274ItWcC:DG3iUXwBUZMX4jee/u7ssX4ItWcC
MD5:	D1725958671FB6996996750B0AE9AE9F
SHA1:	6CA74AEA08CCA32C510BEE358116F03700792D73
SHA-256:	030A3377C2B02B9C9221FB12ECDDAA5055AD7B360D617A5F8C026590ED5A9BAA
SHA-512:	2C528D4FBF09708C18AF9CF931027C9D012F67EB387F2EE2BD8DAB81719CDABE29EDEDCA46E2AA1159829FD22E6A5072DDFD0CBB1E4FD54C0552509F2E1CC1E
Malicious:	false
Reputation:	low
Preview:	..Version.=1.....Event.Type.=A.P.P.C.R.A.S.H.....Event.Time.=1.3.2.6.5.3.8.8.4.0.9.2.7.0.8.0.2.8.....Report.Type.=2.....Consent.=1.....Up.Lo.a.d.T.i.me.=1.3.2.6.5.3.8.8.4.1.0.8.6.4.5.5.4.2.....Report.Status.=2.6.8.4.3.5.4.5.6.....Report.Identifier.=2.6.0.c.6.a.d.1.-d.2.c.e.-4.b.e.1.-b.3.5.4.-5.b.a.0.4.4.9.a.9.1.8.2.....Integrator.Report.Identifier.=a.6.d.f.2.6.8.1.-4.4.5.0.-4.5.9.a.-9.e.f.7.-7.2.1.6.f.c.c.f.f.3.9.e.....Wo.w.6.4.H.o.s.t.=3.4.4.0.4.....Wo.w.6.4.G.uest.=3.3.2.....N.s.App.Name.=r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.1.5.8.4.-0.0.0.1.-0.0.1.7.-f.9.9.8.-e.9.2.5.0.1.4.8.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.3.2.2.2.0.3.4.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\WERBD45.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:06:50 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	57606

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD45.tmp.dmp	
Entropy (8bit):	1.987366736077386
Encrypted:	false
SSDEEP:	192:uyVoozo2TUDgZiu8i5jSjdityAXTw20m8n9nkk:u8h9sj+ejdffw2b8n9kk
MD5:	06ED07EEBD8DC65CBF852E2021BF8BF8
SHA1:	3F2FA511DDEC164E69B77E73C1CFBE8B02EDF421
SHA-256:	ED0FE2F3009B09391CD0D90E7E6EE290699928F719030B653CF77C573D36D85B
SHA-512:	FAAD4EFADEE604FAB55B0F561443AE62396978B69A1704745A4951C8F59EB0AE4F329E1FEA401A530A9555AAA36DAE621E2548C75D2F87EDE2F4F4E4804BFC CA
Malicious:	false
Reputation:	low
Preview:	MDMP.....z2`.....U.....B.....GenuineIntelW.....T.....[2`.....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\WERC19C.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):	3.693397822387037
Encrypted:	false
SSDEEP:	192:Rr17r3GLNid/6aG6Ywq625qGgmfTXVS/CprR389bCmsfdG1Wm:RrlsNi16D6YF62FgmFTFSEoCFFdG9
MD5:	3CE3F5F4CCADF8886692E6C44030658C
SHA1:	98B49C804923F2F336ABE8632E9338CD583CC836
SHA-256:	C65A9E5B7B8AA80E74E2F57F4C54171180759878208F56169C56B27D4F9327E6
SHA-512:	C071B9098CBF848F84B8E7D987178D1528D226ABCB0E1AD8D3786F49F7420A2D8B53A4D27BFFA5F593DCA52389F64955D0E000A1B619067BFC2C8CA01C17967
Malicious:	false
Reputation:	low
Preview:	..<?x.m.l..v.e.r.s.i.o.n.="1...0"..e.n.c.o.d.i.n.g.="U.T.F.-1.6."?>.....<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n>1.0...0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<B.u.i.l.d.>1.7.1.3.4.</B.u.i.l.d.>.....<P.r.o.d.u.c.t>.(0.x.3.0);. W.i.n.d.o.w.s..1.0..P.r.o. </P.r.o.d.u.c.t>.....<E.d.i.t.i.o.n>P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n.>.....<B.u.i.l.d.S.t.r.i.n.g>1.7.1.3.4..1...a.m.d.6.4.f.r.e...r.s.4_..r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4. </B.u.i.l.d.S.t.r.i.n.g.>.....<R.e.v.i.s.i.o.n>1.</R.e.v.i.s.i.o.n>.....<F.l.a.v.o.r>M.u.l.t.i.p.r.o.c.e.s.s.o.r..F.r.e.e.</F.l.a.v.o.r>.....<A.r.c.h.i.t.e.c.t.u.r.e>X.6.4.</ A.r.c.h.i.t.e.c.t.u.r.e>.....<L.C.I.D>1.0.3.3.</L.C.I.D>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<P.i.d>5.5.0.8.</P.i. d>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC2F4.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4663
Entropy (8bit):	4.4744082093595345
Encrypted:	false
SSDEEP:	48:cvlwSD8zsBJgtWi9UqWSC8B78fm8M4JCdsg4NrF2o+q8/d4NfK4SrSP:ulTfT/LSNeJtNp9NuDWPd
MD5:	D1B29C8EE9CBE7A41049F58427AA1415
SHA1:	DB6903F11F54AD98EE38B636D608E0F7A41EC1D5
SHA-256:	42AA2E5316673D64B432AF929AB74EA97ACCF09BC2D5670EA485E0D1B6A8D230
SHA-512:	4C9EF7C51BCE9D4A8BC7353BD3533EE1D3B39441339F9D1AE96A2E10BBB76D4F2B2066B75501B9CD4ECB924842F66CA3D087B38323E3988EBE6A540FD6872B E4
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="987797" />..<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 Wi ndows
------------	--

General	
Entropy (8bit):	7.513886808236697
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:	4e021da2_by_Libranalysis.dll
File size:	167424
MD5:	4e021da22c2701ea547dbd96479f767f
SHA1:	e791b7c6b5b3a98ed405bc5379f3aca438341ed6
SHA256:	e39faf4e4460a28d67296e6ddcff40423569aa45ee7fb6cb68db7014429d8bd6
SHA512:	38b3c61516ffa07952b05171c3f4763946fcec65e778ef2e52e796d80ab73fdbcbbfc73d0fb3d5628a6f9d4cab21014dbf07ec269eb1ede0e375c7143cbec965
SSDEEP:	3072:K9F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj;K9F6rQXvFczvYpQP
File Content Preview:	MZ.....@.....\.....!..L!Th is program cannot be run in DOS mode...\$.Xm.o...< ...<...<U!<...<..B<r...<...<rQ!<...<...<3..<au.<...< szt<"..<Rich...<.....

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x10024cc0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609C7F93 [Thu May 13 01:23:31 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	88962f6760ea005847fb88b87e8ce1fd

Entrypoint Preview

Instruction
mov eax, 00000000h
cmpss xmm1, xmm2, 03h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp eax, 02h
mov eax, ebp
mov dword ptr [10029734h], eax
mov eax, ebx

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.crt	0x28000	0x36b0	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_D ATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x3a0	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_D ATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x26c	0x400	False	0.548828125	data	4.2946697642	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABL E, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Version Infos

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:06:12.084755898 CEST	50200	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:12.149693012 CEST	53	50200	8.8.8.8	192.168.2.3
May 13, 2021 07:06:12.321614027 CEST	51281	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:12.381635904 CEST	53	51281	8.8.8.8	192.168.2.3
May 13, 2021 07:06:12.529730082 CEST	49199	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:12.578414917 CEST	53	49199	8.8.8.8	192.168.2.3
May 13, 2021 07:06:12.882363081 CEST	50620	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:12.933892965 CEST	53	50620	8.8.8.8	192.168.2.3
May 13, 2021 07:06:14.094266891 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:14.145802021 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 07:06:14.971556902 CEST	60152	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:15.023622990 CEST	53	60152	8.8.8.8	192.168.2.3
May 13, 2021 07:06:15.486473083 CEST	57544	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:15.548631907 CEST	53	57544	8.8.8.8	192.168.2.3
May 13, 2021 07:06:16.069029093 CEST	55984	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:16.128964901 CEST	53	55984	8.8.8.8	192.168.2.3
May 13, 2021 07:06:16.975749969 CEST	64185	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:06:17.035387993 CEST	53	64185	8.8.8.8	192.168.2.3
May 13, 2021 07:06:18.088840961 CEST	65110	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:18.137587070 CEST	53	65110	8.8.8.8	192.168.2.3
May 13, 2021 07:06:19.186115980 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:19.234903097 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 07:06:20.090894938 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:20.142101049 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 07:06:21.722460985 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:21.772391081 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 07:06:22.914666891 CEST	60100	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:22.963865995 CEST	53	60100	8.8.8.8	192.168.2.3
May 13, 2021 07:06:24.315103054 CEST	53195	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:24.366724968 CEST	53	53195	8.8.8.8	192.168.2.3
May 13, 2021 07:06:25.178656101 CEST	50141	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:25.235788107 CEST	53	50141	8.8.8.8	192.168.2.3
May 13, 2021 07:06:26.178719044 CEST	53023	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:26.227371931 CEST	53	53023	8.8.8.8	192.168.2.3
May 13, 2021 07:06:27.032063007 CEST	49563	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:27.081860065 CEST	53	49563	8.8.8.8	192.168.2.3
May 13, 2021 07:06:28.539405107 CEST	51352	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:28.589996099 CEST	53	51352	8.8.8.8	192.168.2.3
May 13, 2021 07:06:29.426707983 CEST	59349	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:29.475404024 CEST	53	59349	8.8.8.8	192.168.2.3
May 13, 2021 07:06:30.628009081 CEST	57084	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:30.676721096 CEST	53	57084	8.8.8.8	192.168.2.3
May 13, 2021 07:06:31.866084099 CEST	58823	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:31.914755106 CEST	53	58823	8.8.8.8	192.168.2.3
May 13, 2021 07:06:32.850760937 CEST	57568	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:32.899518013 CEST	53	57568	8.8.8.8	192.168.2.3
May 13, 2021 07:06:44.039997101 CEST	50540	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:44.098830938 CEST	53	50540	8.8.8.8	192.168.2.3
May 13, 2021 07:06:51.825371981 CEST	54366	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:51.874033928 CEST	53	54366	8.8.8.8	192.168.2.3
May 13, 2021 07:06:58.214111090 CEST	53034	53	192.168.2.3	8.8.8.8
May 13, 2021 07:06:58.271070004 CEST	53	53034	8.8.8.8	192.168.2.3
May 13, 2021 07:07:05.327465057 CEST	57762	53	192.168.2.3	8.8.8.8
May 13, 2021 07:07:05.385914087 CEST	53	57762	8.8.8.8	192.168.2.3
May 13, 2021 07:07:07.374015093 CEST	55435	53	192.168.2.3	8.8.8.8
May 13, 2021 07:07:07.432626009 CEST	53	55435	8.8.8.8	192.168.2.3
May 13, 2021 07:07:36.709866047 CEST	50713	53	192.168.2.3	8.8.8.8
May 13, 2021 07:07:36.767180920 CEST	53	50713	8.8.8.8	192.168.2.3
May 13, 2021 07:07:43.456538916 CEST	56132	53	192.168.2.3	8.8.8.8
May 13, 2021 07:07:43.515566111 CEST	53	56132	8.8.8.8	192.168.2.3
May 13, 2021 07:07:59.583046913 CEST	58987	53	192.168.2.3	8.8.8.8
May 13, 2021 07:07:59.654011011 CEST	53	58987	8.8.8.8	192.168.2.3
May 13, 2021 07:08:17.001667023 CEST	56579	53	192.168.2.3	8.8.8.8
May 13, 2021 07:08:17.074435949 CEST	53	56579	8.8.8.8	192.168.2.3
May 13, 2021 07:08:18.848963022 CEST	60633	53	192.168.2.3	8.8.8.8
May 13, 2021 07:08:18.921035051 CEST	53	60633	8.8.8.8	192.168.2.3
May 13, 2021 07:09:04.516415119 CEST	61292	53	192.168.2.3	8.8.8.8
May 13, 2021 07:09:04.616945028 CEST	53	61292	8.8.8.8	192.168.2.3
May 13, 2021 07:09:05.999895096 CEST	63619	53	192.168.2.3	8.8.8.8
May 13, 2021 07:09:06.126808882 CEST	53	63619	8.8.8.8	192.168.2.3
May 13, 2021 07:09:08.066818953 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 07:09:08.128129959 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 07:09:08.629318953 CEST	61946	53	192.168.2.3	8.8.8.8
May 13, 2021 07:09:08.686511040 CEST	53	61946	8.8.8.8	192.168.2.3
May 13, 2021 07:09:09.226380110 CEST	64910	53	192.168.2.3	8.8.8.8
May 13, 2021 07:09:09.284317970 CEST	53	64910	8.8.8.8	192.168.2.3
May 13, 2021 07:09:09.865658998 CEST	52123	53	192.168.2.3	8.8.8.8
May 13, 2021 07:09:09.914448977 CEST	53	52123	8.8.8.8	192.168.2.3
May 13, 2021 07:09:10.437730074 CEST	56130	53	192.168.2.3	8.8.8.8
May 13, 2021 07:09:10.486855984 CEST	53	56130	8.8.8.8	192.168.2.3
May 13, 2021 07:09:11.262085915 CEST	56338	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:09:11.319325924 CEST	53	56338	8.8.8.8	192.168.2.3
May 13, 2021 07:09:12.227264881 CEST	59420	53	192.168.2.3	8.8.8.8
May 13, 2021 07:09:12.280409098 CEST	53	59420	8.8.8.8	192.168.2.3
May 13, 2021 07:09:12.755098104 CEST	58784	53	192.168.2.3	8.8.8.8
May 13, 2021 07:09:12.812491894 CEST	53	58784	8.8.8.8	192.168.2.3

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2021 07:06:12.578414917 CEST	8.8.8.8	192.168.2.3	0x850e	No error (0)	api.global sign.cloud		104.18.24.243	A (IP address)	IN (0x0001)
May 13, 2021 07:06:12.578414917 CEST	8.8.8.8	192.168.2.3	0x850e	No error (0)	api.global sign.cloud		104.18.25.243	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



- loaddll32.exe
- cmd.exe
- rundll32.exe
- WerFault.exe



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5608 Parent PID: 5748

General

Start time:	07:06:19
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\4e021da2_by_Libranalysis.dll'
Imagebase:	0x9a0000
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: 5420 Parent PID: 5608

General

Start time:	07:06:19
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\4e021da2_by_Libranalysis.dll',#1
Imagebase:	0xbd0000
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: 5508 Parent PID: 5420

General

Start time:	07:06:19
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\4e021da2_by_Libranalysis.dll',#1
Imagebase:	0x2e0000
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: 00000002.00000002.285424376.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 2308 Parent PID: 5508

General

Start time:	07:06:48
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5508 -s 764

Imagebase:	0x1160000
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	702B1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD45.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD45.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC2F4.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC2F4.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f8f758f9c9ae6eac81fa9732924e44386348e_82810a17_0958c999	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f8f758f9c9ae6eac81fa9732924e44386348e_82810a17_0958c999\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD45.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC2F4.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD45.tmp.dmp	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC2F4.tmp.xml	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFDF4.tmp.csv	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFE15.tmp.txt	success or wait	1	702A4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD45.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 7a 32 9d 60 a4 05 12 00 00 00 00 00	MDMP z2.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD45.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD45.tmp.dmp	unknown	108	03 00 00 00 f4 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 fc 07 00 00 05 00 00 00 64 01 00 00 a4 36 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 ee c2 00 00 15 00 00 00 ec 01 00 00 84 1d 00 00 16 00 00 00 98 00 00 00 70 1f 00 00	d. ...6.....T.....8..... ...T.....`.....p...	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?.x.m.l..v.e.r.s.i.o.n.=." 1...0". .e.n.c.o.d.i.n.g.=." U.T.F.-.1.6."?>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 35 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.5.0.8.<./P.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 34 00 38 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.0.4.8.4.<./U.p.t.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 33 00 34 00 38 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.3.4.8.1.6.0.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 33 00 33 00 39 00 39 00 36 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.3.3.9.9.6.8.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 30 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.5.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 32 00 34 00 34 00 36 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.4.4.6.7.2.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 32 00 34 00 34 00 36 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.4.4.6.7.2.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.4.1.6.<./Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.1.8.4.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 31 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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.I.U.s.a.g.e>.3.1.1.7.6.<./Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 30 00 39 00 30 00 34 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.I.U.s.a.g.e>.3.0.9.0.4.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 31 00 32 00 39 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e>.6.0.1.2.9.2.8.<./P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 32 00 31 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e>.6.0.2.1.1.2.0.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 31 00 32 00 39 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e>.6.0.1.2.9.2.8.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 34 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d>.5.4.2.0.<./P.i.d>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e>.c.m.d...e.x.e.<./I.m.a.g.e.N.a.m.e>.	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.0.0.0.0.0.0.0.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 38 00 39 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<U.p.t.i.m.e>.3.0.8.9.4.<./U.p.t.i.m.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<I.p.t.E.n.a.b.l.e.d>.0.<./I.p.t.E.n.a.b.l.e.d>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 32 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.>.1.1.2.2.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 31 00 35 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.1.5.0.7.2.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 37 00 38 00 32 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.7.8.2.0.8.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 35 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.4.5.3.5.0.4.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 36 00 33 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.6.3.5.2.0.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 35 00 33 00 35 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.4.5.3.5.0.4.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<P.a.r.a.m.e.t.e.r.0>.r.u.n.d.l.l.3.2...e.x.e.<./P.a.r.a.m.e.t.e.r.0>.	success or wait	8	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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...2.5.6...4.8.<./P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 66 00 68 00 66 00 70 00 79 00 64 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.>.f.h.f.p.y.d.,.I.n.c...<./S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 66 00 68 00 66 00 70 00 79 00 64 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>.f.h.f.p.y.d.7,..1.</.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 31 00 33 00 39 00 37 00 30 00 37 00 31 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>.1.5.8.1.3.9.7.0.7.1.</.O.S.I.n.s.t.a.l.l.D.a.t.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./F.l.a.g.s.>.	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 36 00 3a 00 35 00 30 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.:.0.6:.. 5.0.Z.">.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 34 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 35 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 37 00 34 00 36 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 37 00 34 00 36 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.l.d.= ".3.4.1". .P.I.D.= ".5.5.0.8". .U.p.t.i.m.e.M.S.= ".2.7.4.6.8". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".2.7.4.6.8". .S.u.s.p.e.n.d.e.d.M.S.= ".0". .H.a.n.g.C.o.u.n.t.= ".0". .G.h.o.s.t.C.o.u.n.t.= ".0". .C.r.a.s.h.e.d	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 36 00 30 00 63 00 36 00 61 00 64 00 31 00 2d 00 64 00 32 00 63 00 65 00 2d 00 34 00 62 00 65 00 31 00 2d 00 62 00 33 00 35 00 34 00 2d 00 35 00 62 00 61 00 30 00 34 00 34 00 39 00 61 00 39 00 31 00 38 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.2.6.0.c.6.a.d.1-.d.2.c.e.-.4.b.e.1-.b.3.5.4-.5.b.a.0.4.4.9.a.9.1.8.2.<./G.u.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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 36 00 3a 00 35 00 30 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.:.0.6.:.5.0.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC19C.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC2F4.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">.. <tim>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f8f758f9c9ae6eac81fa9732924e44386348e_82810a17_0958c999\Report.wer	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f8f758f9c9ae6eac81fa9732924e44386348e_82810a17_0958c999\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	182	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f8f758f9c9ae6eac81fa9732924e44386348e_82810a17_0958c999\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 34 00 39 00 36 00 34 00 32 00 31 00 39 00 33 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.4. 9.6.4.2.1.9.3.5.	success or wait	1	702A497A	unknown

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRYA\{8fe76050-c43c-6af5-6969-2194037a0be3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRYA\{8fe76050-c43c-6af5-6969-2194037a0be3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRYA\{8fe76050-c43c-6af5-6969-2194037a0be3}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	702C36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	702C1FB2	RegCreateKeyExW
\REGISTRYA\{8fe76050-c43c-6af5-6969-2194037a0be3}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702A43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{8fe76050-c43c-6af5-6969-2194037a0be3}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519fec486de87ed73cb92d3cac802400000000	success or wait	1	702C36BF	unknown
\REGISTRYA\{8fe76050-c43c-6af5-6969-2194037a0be3}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	702C36BF	unknown

