

JOeSandbox Cloud BASIC



ID: 413060

Sample Name:

0f72be74_by_Libranalysis

Cookbook: default.jbs

Time: 07:17:40

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 0f72be74_by_Libranalysis	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Dridex	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Networking:	5
E-Banking Fraud:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
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	10
JA3 Fingerprints	11
Dropped Files	12
Created / dropped Files	12
Static File Info	13
General	13
File Icon	13
Static PE Info	13
General	14
Entrypoint Preview	14
Rich Headers	14
Data Directories	15
Sections	15
Resources	15
Imports	15
Version Infos	15
Network Behavior	16
UDP Packets	16

Code Manipulations	17
Statistics	17
Behavior	17
System Behavior	17
Analysis Process: loadll32.exe PID: 5520 Parent PID: 5700	18
General	18
File Activities	18
Analysis Process: cmd.exe PID: 5752 Parent PID: 5520	18
General	18
File Activities	18
Analysis Process: rundll32.exe PID: 5056 Parent PID: 5752	18
General	18
Analysis Process: WerFault.exe PID: 6944 Parent PID: 5056	19
General	19
File Activities	19
File Created	19
File Deleted	19
File Written	20
Registry Activities	41
Key Created	41
Key Value Created	41
Disassembly	42
Code Analysis	42

Analysis Report 0f72be74_by_Libranalysis

Overview

General Information

Sample Name:

0f72be74_by_Libranalysis
(renamed file extension from none to dll)

Analysis ID:

413060

MD5:

0f72be74fa3f62c...

SHA1:

66925350b9c8d0..

SHA256:

3078512d8dc554..

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Dridex

Score:

64

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

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 DirectInput object (often fo...

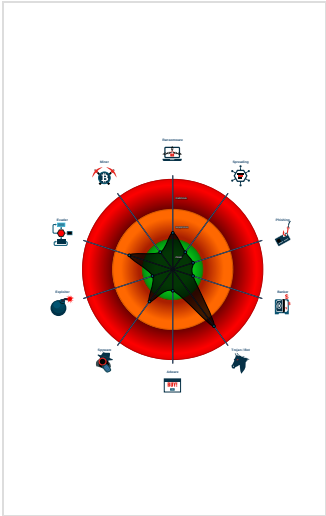
Creates a process in suspended mo...

Detected potential crypto function

IP address seen in connection with o...

Internet Provider seen in connection...

Classification



Startup

System is w10x64

loadall32.exe (PID: 5520 cmdline: loadall32.exe 'C:\Users\user\Desktop\0f72be74_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 5752 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0f72be74_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 5056 cmdline: rundll32.exe 'C:\Users\user\Desktop\0f72be74_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 6944 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5056 -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": [
    "16dkGS0zdHgjuCcIXGdSX7UrHwfYsUG8wEUtKNgzHrWMfTGafJbc",
    "39t3NdDhurvp1tFNCpVA5goSy1kxj1BtIwMPTv1DPbNEcuIekQC70"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.333090101.0000000010001000.00000020.00020000.sdm	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Copyright Joe Security LLC 2021

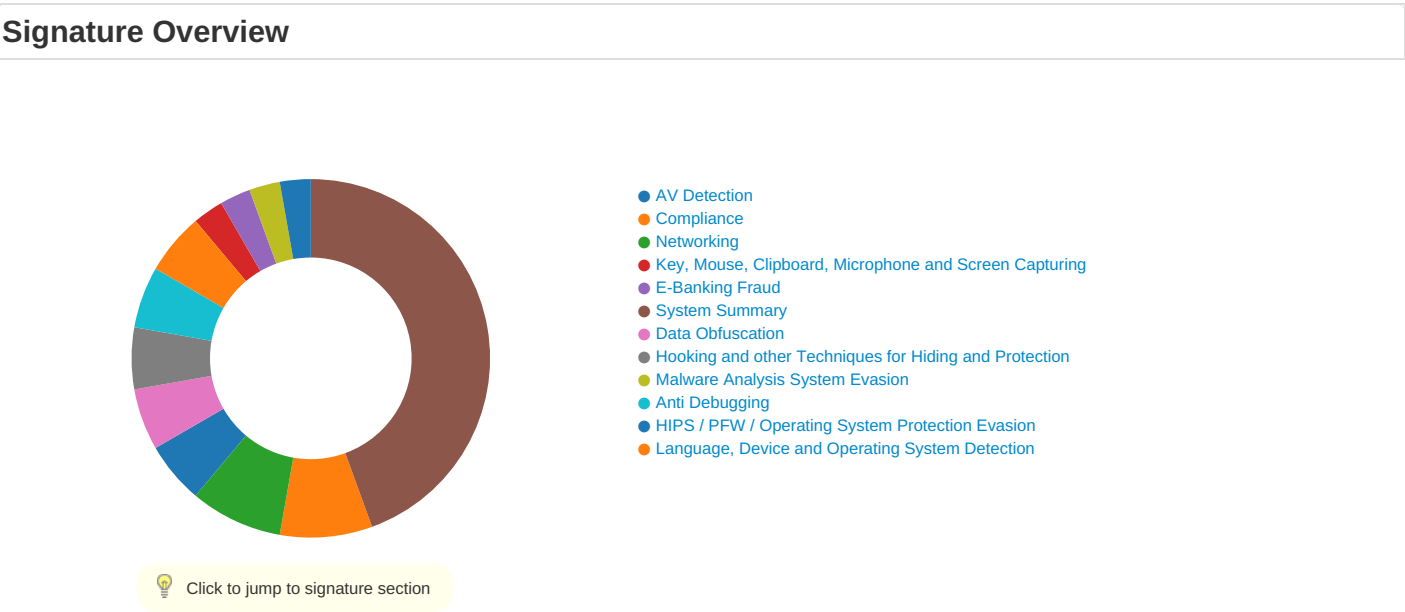
Page 4 of 42

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



AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

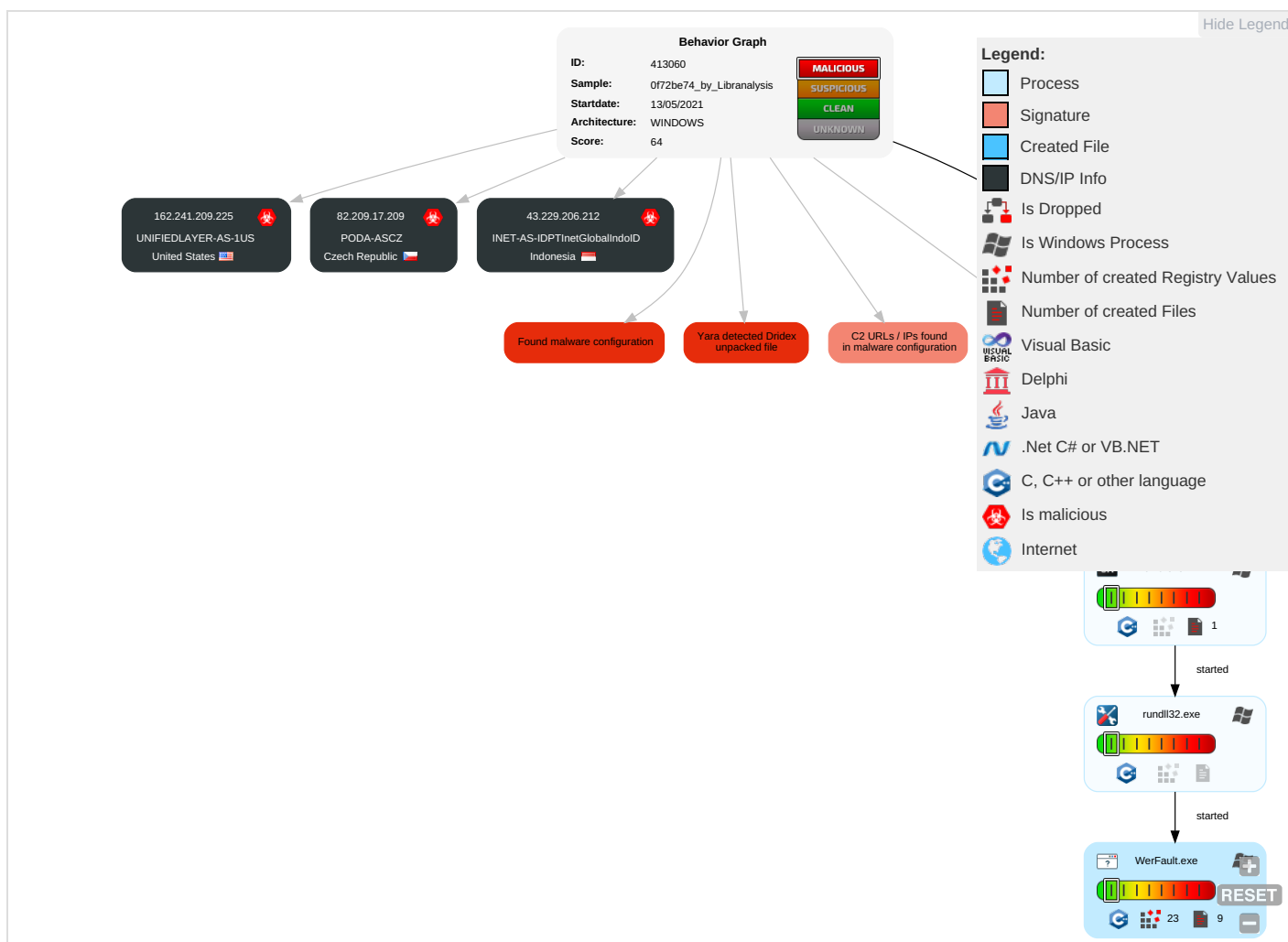
Yara detected Dridex unpacked file

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	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

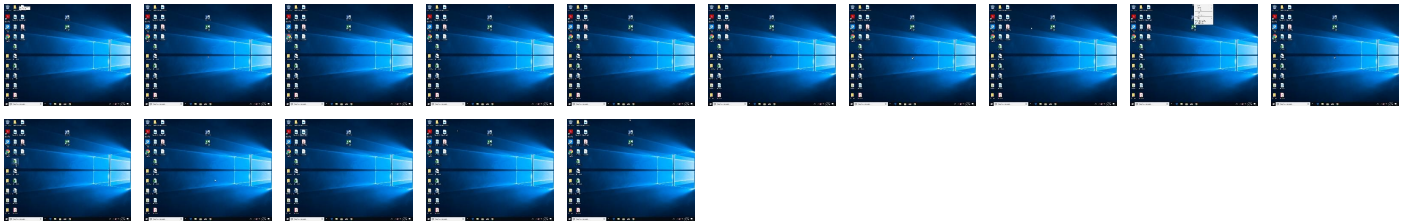
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
0f72be74_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.a40000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

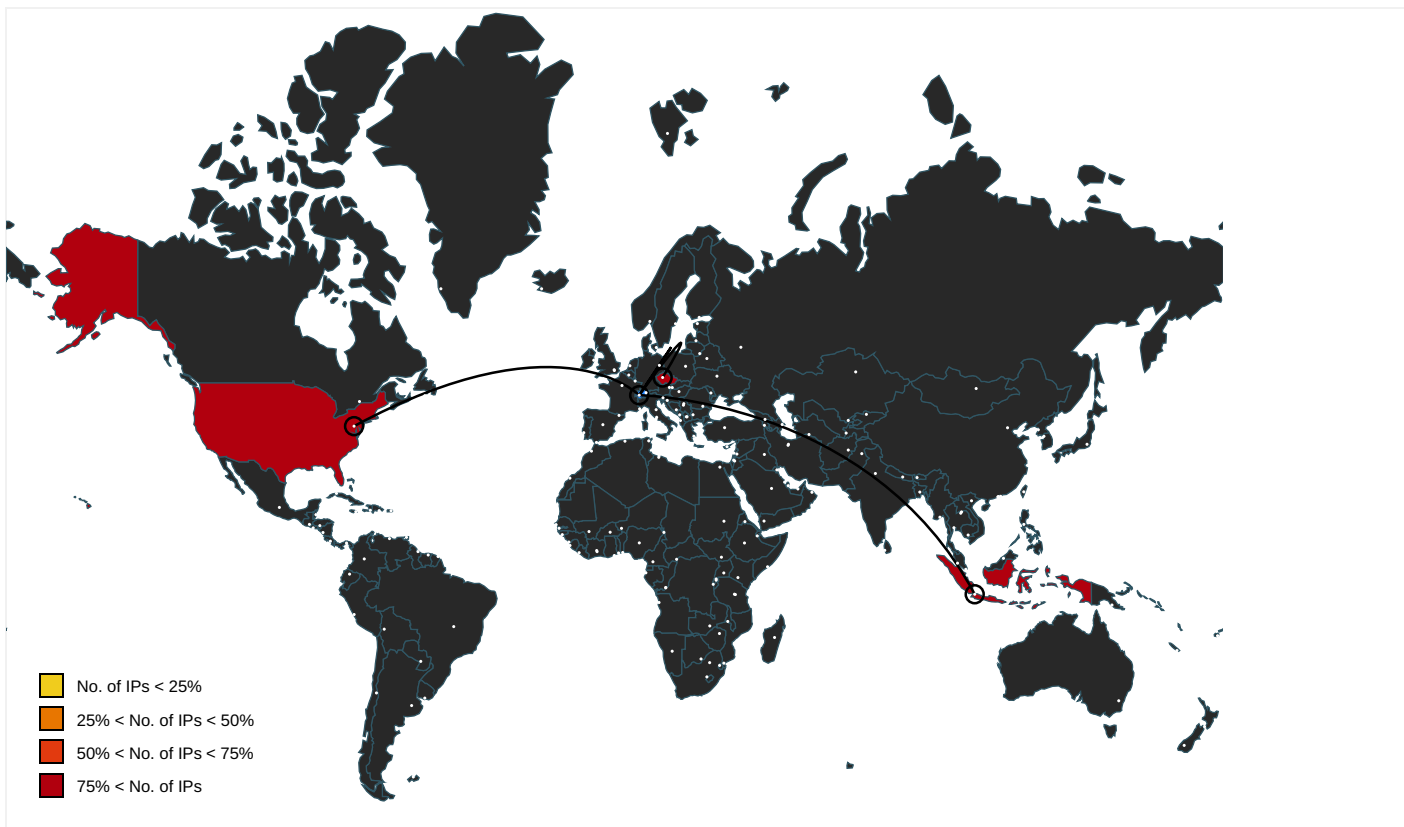
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

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:	413060
Start date:	13.05.2021
Start time:	07:17:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 38s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	0f72be74_by_Libranalysis (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.5% (good quality ratio 85.2%) • Quality average: 67.1% • Quality standard deviation: 35%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Simulations

Behavior and APIs

Time	Type	Description
07:19:14	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.209.225	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	
43.229.206.212	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
INET-AS-IDPTInetGlobalIndoID	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	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
UNIFIEDLAYER-AS-1US	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	86fa0c16_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
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	4e021da2_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
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	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
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_41fa1884768d4e739447e9cfb8aa8e7080fe54_82810a17_1b797176\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12488
Entropy (8bit):	3.7667939984654675
Encrypted:	false
SSDEEP:	192:t8iW0oXT0cHBUZMX4jed+Fe/u7sMS274ItWcT:yiQXTPBUZMX4jex/u7sMX4ItWcT
MD5:	A44B10F8AB1D2FC02922223172C0AB51
SHA1:	3D5DA9D6C9BA438D2630571BCBF2D793D0958FD8
SHA-256:	6FB13367B65C29ECF10A31F6E810B759A391900FEFB93333F059266FBAA2BD74
SHA-512:	F78822A9DE79302AA9098021240E1FC980A153890DB9F345EDE29E9EF36F98C1E5A97F9B24ABEB5CAF3E3500224EC2DE7B7AD06495028F53C6FEC0A05A39ED7F
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=1.3.2.6.5.3.8.9.1.4.4.0.9.1.5.5.9.5.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....U.p.l.o.a.d.T.i.m.e.=1.3.2.6.5.3.8.9.1.5.2.9.3.5.2.8.2.7.....R.e.p.o.r.t.S.t.a.t.u.s.=2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=a.f.e.8.3.f.f.c.-5.7.0.a.-4.1.d.3.-b.d.a.b.-1.1.0.9.1.1.5.7.0.8.5.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=c.d.5.f.1.1.3.1.-4.f.e.a.-4.c.9.f.-9.f.c.7.-e.f.7.6.e.4.b.5.7.0.5.c.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.1.3.c.0.-0.0.0.1.-0.0.1.7.-d.e.4.a.-6.4.d.a.0.2.4.8.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.8.0.2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.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\WER46DB.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:19:07 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45518
Entropy (8bit):	2.151934227806914
Encrypted:	false
SSDEEP:	192:jQTYdcTnTs+UY9hO4Jir9aXqZVtsDqtUTRmrSDn3EohdxS2cciiir8hw:FcTy+UY9hOE094GxtkRmuDn0SDS2zYhw
MD5:	443F1F21079BECCED9EF0545F31012E9
SHA1:	DF06FD6F49AECAA1F8363113909EF8C7AE80BC45
SHA-256:	692ECA5CA97A26AFE2EB0505523944ED99F8F7EA01093C1C76058241D6F4EBA9
SHA-512:	A179A66EFF591A63353674E0801730C6166B081AFC67494F9C990F630693B0AE2E8CB05C62EDAA97473D9935E7EE5866047656C60E6EE3FB021D16FD5FA6BE83
Malicious:	false
Reputation:	low
Preview:	MDMP.....[5`.....U.....B.....GenuineIntelW.....T.....85`.....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\WER5302.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):	3.692906936804647
Encrypted:	false
SSDEEP:	192:RrI7r3GLNibnz6a6Ye565GgmfTIVS/Cpr/89bwbZsf0n2jm:RrlsNi/6a6YY65GgmfTvSHwbyfb6
MD5:	56C645D3403C7DAFEF3F6D341BDF9A4A
SHA1:	FB6CEF5D2F214AF584D246F373C1D00D4D61D80B
SHA-256:	6CA61D1DEAA7D00D38DD417BEDF05C0BBAD84611F4B0C47514B12A4B67879102
SHA-512:	F86CA5C811D01FCA92CC9374E56230504AA05EA0AC0299391A9218386446730CD5BC34D855D223C0DB057A84714BA91C63565E3F09818E8D091D854D74E8A287
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	
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.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.>5.0.5.6.</P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5583.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):	4.4676372560772215
Encrypted:	false
SSDEEP:	48:cvlwSD8zsvJgtWI9OYWSC8Bp8fm8M4JCdshNrFv+q8/4NFO4SrS0d:ulTfRJRSN0JXNlnNADW0d
MD5:	12E8E52884FD543A5D5CFBB4C1AA9F5B
SHA1:	BC0FC105AB849840757F752B602A3962FA47AFA7
SHA-256:	C00CBF6423191ED234F24DD8E6DDE1CB36150E432441BA01A7F3215A9DEC8272
SHA-512:	8064140DFF930BB16DD1F1C13F8C8F1D2509A3299B3838E42B808AC701805F7BAD93EA2B10EAD7FD962601BC60C2D1816A0BF3E0F79DA3B6D2FFAAA2417BF210
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="987809" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.513868857555084
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:	0f72be74_by_Libranalysis.dll
File size:	167424
MD5:	0f72be74fa3f62cdc228d4c3b5d84406
SHA1:	66925350b9c8d0919d6eebd6efeab17edac1a3cd
SHA256:	3078512d8dc5547c01c07d044be234a69e79456b0480dc6d8cbf5354b52021e
SHA512:	ce6dace2f465a9886aed7d7f6a099f33d1eeb29acdef9d2ed71be0cff745d866ca9baf1fb4447ce539eeb833e588c33a74f436931c3ae70ddc326bef75d002d4
SSDEEP:	3072:d9F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:d9F6rQXvFczyYpQP
File Content Preview:	MZ.....@.....\.....!..L!Th is program cannot be run in DOS mode...\$.....Xm.o...<...<...<U!<...<.B<r...<...<rQ!<...<...<...<3..<au.<...<sz!<...<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:	0x609C8024 [Thu May 13 01:25:56 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

[illegible]

Rich Headers

Programming Language:	• [RES] VS2015 build 23026 • [IMP] VS2013 UPD4 build 31101 • [C] VS2010 build 30319 • [RES] VS2015 UPD2 build 23918 • [C++] VS2005 build 50727 • [IMP] VS2010 SP1 build 40219 • [RES] VS2012 build 50727
-----------------------	--

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2770a	0x5b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x277d8	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x1220	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10018	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x4c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x23dfe	0x23e00	False	0.756362968206	data	7.53078515147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2ceb	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x331c	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0xe88	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x26c	0x400	False	0.548828125	data	4.2946697642	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Version Infos

Description	Data
LegalCopyright	Copyright 2018
InternalName	x2otfb
FileVersion	7.2.5422.00

Description	Data
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 07:18:24.298969984 CEST	58562	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:24.347706079 CEST	53	58562	8.8.8.8	192.168.2.7
May 13, 2021 07:18:25.092588902 CEST	56590	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:25.141499043 CEST	53	56590	8.8.8.8	192.168.2.7
May 13, 2021 07:18:26.584249020 CEST	60501	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:26.632965088 CEST	53	60501	8.8.8.8	192.168.2.7
May 13, 2021 07:18:27.441502094 CEST	53775	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:27.491456985 CEST	53	53775	8.8.8.8	192.168.2.7
May 13, 2021 07:18:28.703207970 CEST	51837	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:28.754823923 CEST	53	51837	8.8.8.8	192.168.2.7
May 13, 2021 07:18:29.047719002 CEST	55411	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:29.106168985 CEST	53	55411	8.8.8.8	192.168.2.7
May 13, 2021 07:18:29.725989103 CEST	63668	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:29.783138990 CEST	53	63668	8.8.8.8	192.168.2.7
May 13, 2021 07:18:31.074894905 CEST	54640	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:31.126477957 CEST	53	54640	8.8.8.8	192.168.2.7
May 13, 2021 07:18:31.923074961 CEST	58739	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:31.971919060 CEST	53	58739	8.8.8.8	192.168.2.7
May 13, 2021 07:18:33.361898899 CEST	60338	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:33.412208080 CEST	53	60338	8.8.8.8	192.168.2.7
May 13, 2021 07:18:36.136373997 CEST	58717	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:36.185132027 CEST	53	58717	8.8.8.8	192.168.2.7
May 13, 2021 07:18:37.613775015 CEST	59762	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:37.665333986 CEST	53	59762	8.8.8.8	192.168.2.7
May 13, 2021 07:18:38.485734940 CEST	54329	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:38.536078930 CEST	53	54329	8.8.8.8	192.168.2.7
May 13, 2021 07:18:39.734210014 CEST	58052	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:39.787527084 CEST	53	58052	8.8.8.8	192.168.2.7
May 13, 2021 07:18:40.635524035 CEST	54008	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:40.685038090 CEST	53	54008	8.8.8.8	192.168.2.7
May 13, 2021 07:18:41.829571962 CEST	59451	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:41.878415108 CEST	53	59451	8.8.8.8	192.168.2.7
May 13, 2021 07:18:43.148817062 CEST	52914	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:43.197487116 CEST	53	52914	8.8.8.8	192.168.2.7
May 13, 2021 07:18:44.699552059 CEST	64569	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:44.748260021 CEST	53	64569	8.8.8.8	192.168.2.7
May 13, 2021 07:18:45.511657953 CEST	52816	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:45.561816931 CEST	53	52816	8.8.8.8	192.168.2.7
May 13, 2021 07:18:48.763027906 CEST	50781	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:48.824951887 CEST	53	50781	8.8.8.8	192.168.2.7
May 13, 2021 07:18:50.106645107 CEST	54230	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:50.155375004 CEST	53	54230	8.8.8.8	192.168.2.7
May 13, 2021 07:18:51.851288080 CEST	54911	53	192.168.2.7	8.8.8.8
May 13, 2021 07:18:51.899980068 CEST	53	54911	8.8.8.8	192.168.2.7
May 13, 2021 07:19:13.122421026 CEST	49958	53	192.168.2.7	8.8.8.8
May 13, 2021 07:19:13.195455074 CEST	53	49958	8.8.8.8	192.168.2.7
May 13, 2021 07:19:14.360444069 CEST	50860	53	192.168.2.7	8.8.8.8
May 13, 2021 07:19:14.411690950 CEST	53	50860	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:19:20.043849945 CEST	50452	53	192.168.2.7	8.8.8.8
May 13, 2021 07:19:20.095061064 CEST	53	50452	8.8.8.8	192.168.2.7
May 13, 2021 07:19:21.414180994 CEST	59730	53	192.168.2.7	8.8.8.8
May 13, 2021 07:19:21.472861052 CEST	53	59730	8.8.8.8	192.168.2.7
May 13, 2021 07:19:53.675729036 CEST	59310	53	192.168.2.7	8.8.8.8
May 13, 2021 07:19:53.746349096 CEST	53	59310	8.8.8.8	192.168.2.7
May 13, 2021 07:20:01.643136978 CEST	51919	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:01.701373100 CEST	53	51919	8.8.8.8	192.168.2.7
May 13, 2021 07:20:17.941777945 CEST	64296	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:17.990458965 CEST	53	64296	8.8.8.8	192.168.2.7
May 13, 2021 07:20:18.518970013 CEST	56680	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:18.577477932 CEST	53	56680	8.8.8.8	192.168.2.7
May 13, 2021 07:20:19.188913107 CEST	58820	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:19.250957012 CEST	53	58820	8.8.8.8	192.168.2.7
May 13, 2021 07:20:19.295464039 CEST	60983	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:19.361222982 CEST	53	60983	8.8.8.8	192.168.2.7
May 13, 2021 07:20:19.682565928 CEST	49247	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:19.739543915 CEST	53	49247	8.8.8.8	192.168.2.7
May 13, 2021 07:20:20.333023071 CEST	52286	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:20.390700102 CEST	53	52286	8.8.8.8	192.168.2.7
May 13, 2021 07:20:21.174401045 CEST	56064	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:21.223011971 CEST	53	56064	8.8.8.8	192.168.2.7
May 13, 2021 07:20:22.075489998 CEST	63744	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:22.138040066 CEST	53	63744	8.8.8.8	192.168.2.7
May 13, 2021 07:20:23.427648067 CEST	61457	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:23.476398945 CEST	53	61457	8.8.8.8	192.168.2.7
May 13, 2021 07:20:24.690454006 CEST	58367	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:24.742062092 CEST	53	58367	8.8.8.8	192.168.2.7
May 13, 2021 07:20:25.265427113 CEST	60599	53	192.168.2.7	8.8.8.8
May 13, 2021 07:20:25.322405100 CEST	53	60599	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: loadll32.exe PID: 5520 Parent PID: 5700**General**

Start time:	07:18:31
Start date:	13/05/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\0f72be74_by_Libranalysis.dll'
Imagebase:	0x20000
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: 5752 Parent PID: 5520**General**

Start time:	07:18:31
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\0f72be74_by_Libranalysis.dll',#1
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: rundll32.exe PID: 5056 Parent PID: 5752**General**

Start time:	07:18:32
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\0f72be74_by_Libranalysis.dll',#1
Imagebase:	0xd50000
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: 00000002.00000002.333090101.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6944 Parent PID: 5056

General

Start time:	07:19:02
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5056 -s 764
Imagebase:	0xb80000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D251717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5583.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5583.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_41fa1884768d4e739447e9cfb8aa8e7080fe54_82810a17_1b797176	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_41fa1884768d4e739447e9cfb8aa8e7080fe54_82810a17_1b797176\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp	success or wait	1	6D24497A	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5583.tmp	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp.dmp	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5583.tmp.xml	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER55C0.tmp.csv	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER597A.tmp.txt	success or wait	1	6D244BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 5b 35 9d 60 a4 05 12 00 00 00 00 00	MDMP.....[5.`.....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 a8 1f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 c0 13 00 00 38 35 9d 60 07 00 00 00 11 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	U.....B..... ..GenuineIntelW.....T..85`.....0.=..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	...r.u.n.d.l.l.3.2...e.x.e...	success or wait	51	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp.dmp	unknown	752	00 00 93 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 62 25 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 20 57 02 00 00 00 00 00 b0 d3 02 00 00 00 00 8a 4b 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 5f e7 00 00 00 00 00 00 9e 4b 03 00 00 00 00 00 e2 95 02 00 00 00 00 00 ff ff ff 00 00 00 00 f4 f2 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 e2 26 22 00 00 00 00	...s....0...U..s@..b%.....B.....B?.....#..... ..@A.....Zb..... W..... ..K....._.....K!..... @.....&"....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	E.v.e.n.t.....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.I.R.T.i.m	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER46DB.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 9c 07 00 00 05 00 00 00 f4 00 00 00 ac 30 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 b6 93 00 00 15 00 00 00 ec 01 00 00 24 1d 00 00 16 00 00 00 98 00 00 00 10 1f 00 00	0.....T.....8..... ...T..... ..\$.....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	<?.xml..version="1.0". encoding="UTF-16"?>	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n>1.0...0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n>	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<B.u.i.l.d.>1.7.1.3.4.</B.u.i.l.d.>	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t>.(.0.x.3.0.). :. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./P.r.o.d.u.c.t>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n>.P.r.o.f.e.s.s.i.o.n.a.l.<./E.d.i.t.i.o.n>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.<./B.u.i.l.d.S.t.r.i.n.g>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n>.1.<./R.e.v.i.s.i.o.n>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./F.l.a.v.o.r>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./L.C.I.D.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 30 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.0.5.6.<./P.i.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 35 00 31 00 30 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.5.1.0.8.<./U.p.t.i.m.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4.g.u.e.s.t.=."3.3.2".h.o.s.t.=."3.4.4.0.4".>.1.<./W.o.w.6.4.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 32 00 39 00 39 00 35 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.2.9.9.5.8.4.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 37 00 32 00 39 00 31 00 33 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.>.1.2.7.2.9.1.3.9.2.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 38 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.6.8.9.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 32 00 34 00 31 00 39 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.>.9.2.2.4.1.9.2.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 31 00 39 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.>.9.2.2.4.1.9.2.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 36 00 34 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.>.1.8.4.6.4.0.<./Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 30 00 32 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.3.0.2.4.8.<./.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 39 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 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>.2.9.9.7.6.<./.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 39 00 31 00 37 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e>.5.7.9.1.7.4.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 39 00 39 00 39 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.7.9.9.3.6.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 39 00 31 00 37 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.7.9.1.7.4.4.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.7.5.2.<./P.i.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.l.m.a.g.e.N.a.m.e.>.c.m.d...e.x.e.<./l.m.a.g.e.N.a.m.e.>.	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 35 00 34 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<U.p.t.i.m.e>.3.5.4.7.0.<./U.p.t.i.m.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<W.o.w.6.4.g.u.e.s.t>="3.3.2".h.o.s.t="3.4.4.0.4".>.1.<./W.o.w.6.4>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<I.p.t.E.n.a.b.l.e.d>.0.<./I.p.t.E.n.a.b.l.e.d>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 32 00 33 00 32 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.2.3.2.6.4.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 38 00 36 00 34 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.8.6.4.0.0.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.4.0.9.6.0.<./Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.3.3.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.4.9.5.2.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 33 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.3.4.7.2.0.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 39 00 32 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.9.2.1.9.2.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 33 00 34 00 37 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.3.4.7.2.0.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./E.v.e.n.t.T.y.p.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<P.a.r.a.m.e.t.e.r.0>.r.u.n.d.l.l.3.2...e.x.e.<./P.a.r.a.m.e.t.e.r.0>.	success or wait	8	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./M.I.D.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 72 00 61 00 6c 00 6e 00 6c 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.>.r.r.a.l.n.l.,.l.n.c...<./S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 72 00 72 00 61 00 6c 00 6e 00 6c 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>.r.r.a.l.n.l.7.,,1.</.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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.</.B.I.O.S.V.e.r.s.i.o.n>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 38 00 30 00 35 00 33 00 30 00 35 00 37 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e>.1.5.6.8.0.5.3.0.5.7.</.O.S.I.n.s.t.a.l.l.D.a.t.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:2.1.Z.</.O.S.I.n.s.t.a.l.l.T.i.m.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./I.n.t.e.g.r.a.t.o.r.>	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 31 00 39 00 3a 00 30 00 37 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.:1.9:.. 0.7.Z.">	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 30 00 35 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 38 00 36 00 32 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 38 00 36 00 32 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 32 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.i.d.= ".3.4.0". .P.I.D.= ".5.0.5.6". .U.p.t.i.m.e.M.S.= ".2.8.6.2.4". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".2.8.6.2.4". .S.u.s.p.e.n.d.e.d.M.S.= ".0". .H.a.n.g.C.o.u.n.t.= ".0". .G.h.o.s.t.C.o.u.n.t.= ".0". .C.r.a.s.h.e.d	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./P.r.o.c.e.s.s.>	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 66 00 65 00 38 00 33 00 66 00 66 00 63 00 2d 00 35 00 37 00 30 00 61 00 2d 00 34 00 31 00 64 00 33 00 2d 00 62 00 64 00 61 00 62 00 2d 00 31 00 31 00 30 00 39 00 31 00 31 00 35 00 37 00 30 00 38 00 35 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.a.f.e.8.3.f.f.c.-.5.7.0.a.-.4.1.d.3.-.b.d.a.b.-.1.1.0.9.1.1.5.7.0.8.5.7.<./G.u.i.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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 31 00 39 00 3a 00 30 00 37 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.-.1.9.:0.7.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5302.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5583.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_41fa1884768d4e739447e9cfb8aa8e7080fe54_82810a17_1b797176\Report.wer	unknown	2	ff fe	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_41fa1884768d4e739447e9cfb8aa8e7080fe54_82810a17_1b797176\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	182	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_41fa1884768d4e739447e9cfb8aa8e7080fe54_82810a17_1b797176\Report.wer	unknown	46	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 32 00 31 00 30 00 36 00 31 00 39 00 34 00 34 00 38 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.2. 1.0.6.1.9.4.4.8.9.	success or wait	1	6D24497A	unknown

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRYA\{a1070a4d-21e3-4db6-3809-6353fc6c2579}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2636BF	unknown
\REGISTRYA\{a1070a4d-21e3-4db6-3809-6353fc6c2579}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2636BF	unknown
\REGISTRYA\{a1070a4d-21e3-4db6-3809-6353fc6c2579}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D2636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D261FB2	RegCreateKeyExW
\REGISTRYA\{a1070a4d-21e3-4db6-3809-6353fc6c2579}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{a1070a4d-21e3-4db6-3809-6353fc6c2579}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519fec486de87ed73cb92d3cac802400000000	success or wait	1	6D2636BF	unknown
\REGISTRYA\{a1070a4d-21e3-4db6-3809-6353fc6c2579}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D2636BF	unknown

