

JoeSandbox Cloud BASIC



ID: 413036

Sample Name:

0f6f2d53_by_Libranalysis.dll

Cookbook: default.jbs

Time: 06:50:01

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 0f6f2d53_by_Libranalysis.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Dridex	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Networking:	5
E-Banking Fraud:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
Contacted IPs	8
Public	8
General Information	8
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	10
ASN	10
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	13
General	13
File Icon	13
Static PE Info	14
General	14
Entrypoint Preview	14
Rich Headers	15
Data Directories	15
Sections	15
Resources	15
Imports	15
Version Infos	16
Network Behavior	16
UDP Packets	16

Code Manipulations	17
Statistics	17
Behavior	17
System Behavior	18
Analysis Process: loadll32.exe PID: 4660 Parent PID: 5624	18
General	18
File Activities	18
Analysis Process: cmd.exe PID: 5396 Parent PID: 4660	18
General	18
File Activities	18
Analysis Process: rundll32.exe PID: 4604 Parent PID: 5396	18
General	18
Analysis Process: WerFault.exe PID: 5672 Parent PID: 4604	19
General	19
File Activities	19
File Created	19
File Deleted	20
File Written	20
Registry Activities	41
Key Created	41
Key Value Created	41
Disassembly	42
Code Analysis	42

Analysis Report 0f6f2d53_by_Libranalysis.dll

Overview

General Information

Sample Name:

0f6f2d53_by_Libranalysis.dll

Analysis ID:

413036

MD5:

0f6f2d53b1f7eb7...

SHA1:

8032adfd6cef055..

SHA256:

2cfd348c1d4dcc5..

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Dridex

Score:

72

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected Dridex unpacked file

C2 URLs / IPs found in malware con...

Machine Learning detection for samp...

Checks if the current process is bein...

Contains functionality to check if a d...

Contains functionality to query locale...

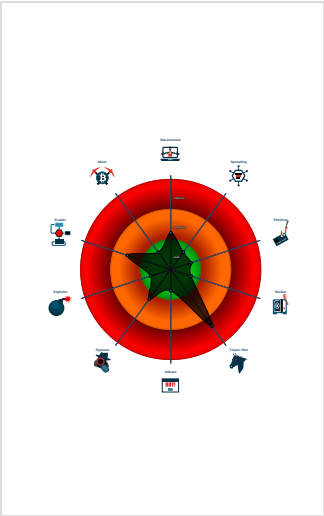
Creates a process in suspended mo...

Detected potential crypto function

IP address seen in connection with o...

Internet Provider seen in connection...

Classification



Startup

System is w10x64

loaddll32.exe (PID: 4660 cmdline: loaddll32.exe 'C:\Users\user\Desktop\0f6f2d53_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 5396 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0f6f2d53_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 4604 cmdline: rundll32.exe 'C:\Users\user\Desktop\0f6f2d53_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 5672 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4604 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

cleanup

Malware Configuration

Threatname: Dridex

```
{
  "Version": 22202,
  "C2 list": [
    "43.229.206.212:443",
    "82.209.17.209:8172",
    "162.241.209.225:4125"
  ],
  "RC4 keys": [
    "16dkGS0zdHgjuCciXGd5X7UrHwFYsUG8wEUtKNgzHrWMfTGafJbC",
    "UlufoCqJDohDzG0dBY6ldd1IbFW5KV8BqCAnkqwdZvq0CsZ00ngL"
  ]
}
```

Yara Overview

Memory Dumps

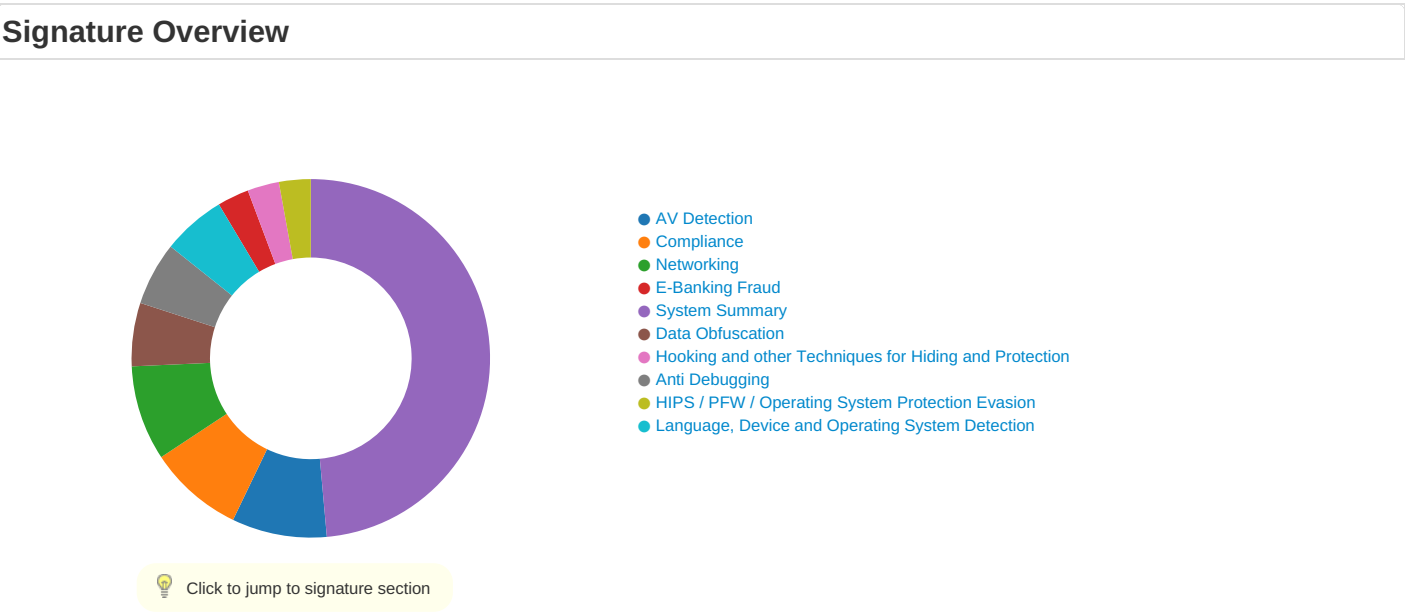
Source	Rule	Description	Author	Strings
00000003.00000002.275435929.0000000010001000.00000020.00020000.sdmf	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

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

Sigma Overview

No Sigma rule has matched



AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

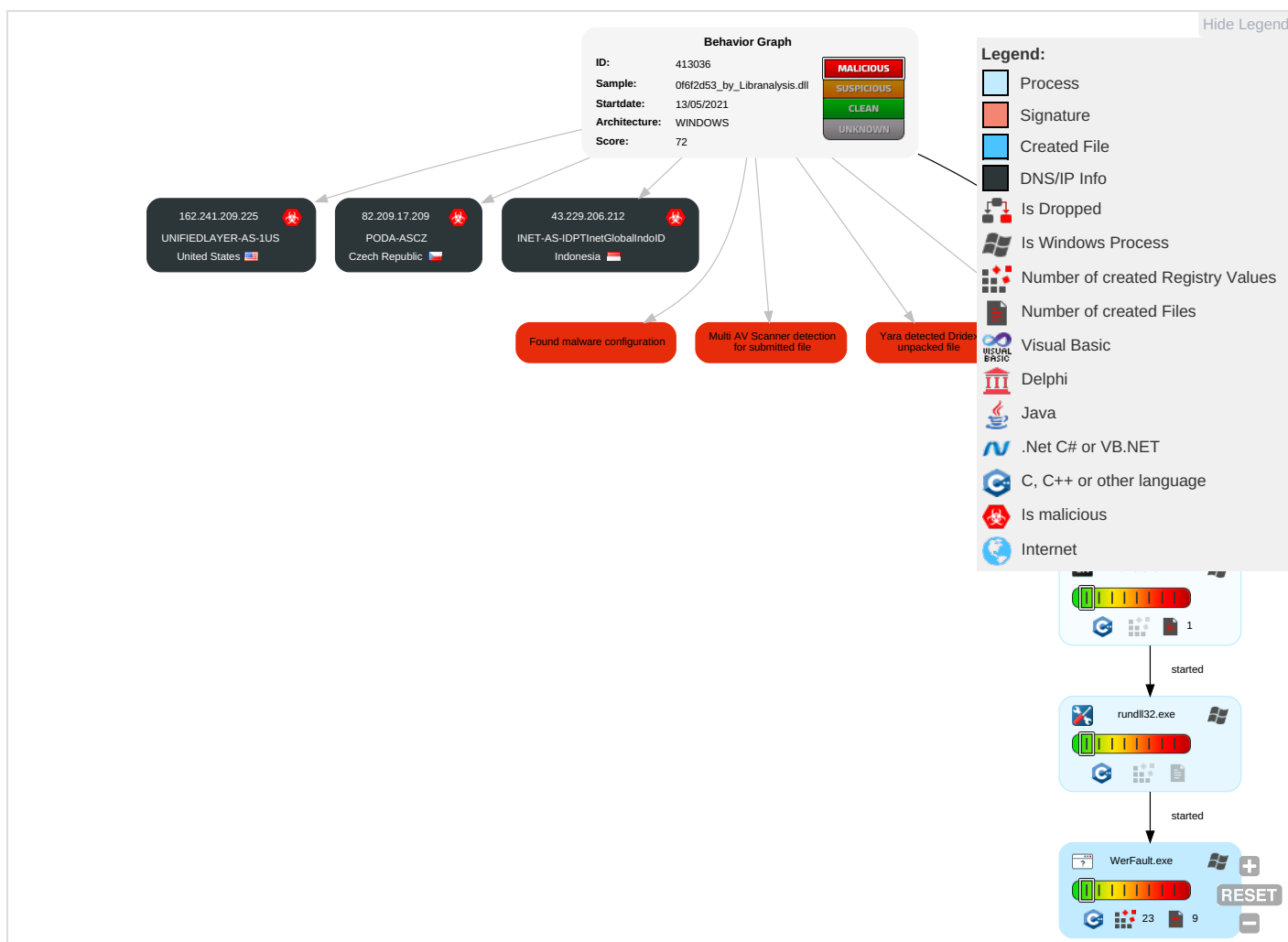
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

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

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

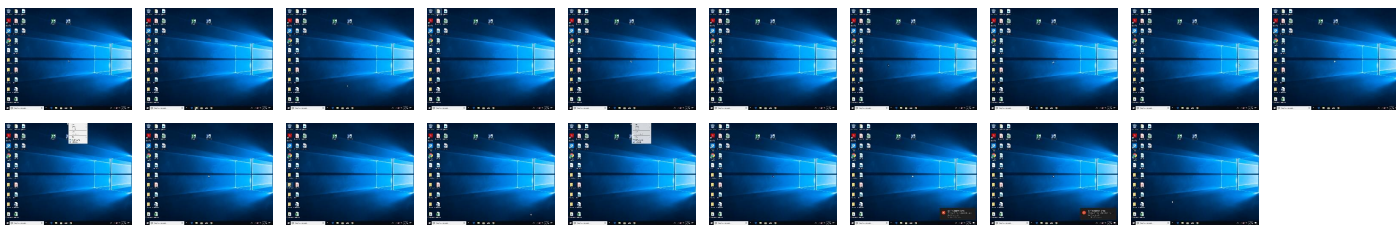
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
0f6f2d53_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
0f6f2d53_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.b00000.2.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:	413036
Start date:	13.05.2021
Start time:	06:50:01
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 6m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0f6f2d53_by_Libranalysis.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 60.8% (good quality ratio 51.1%) • Quality average: 62.9% • Quality standard deviation: 37.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	0ee1d71e_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
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	
SSDEEP:	192:RrI7r3GLNioMt6s+6YSG6NgmfT8LSoCpr989b5ysf690Tm:RrlsNix6t6Yr6NgmfTGSK5xfi
MD5:	C18C159A4E63A641C4A6466FD2CE2EFB
SHA1:	21B77EE96DEAD8C02FC0CFABBC729D1FFE9D4E3A
SHA-256:	61E9CC27FD1D0172749B9159C7BDE7CF707635F4282AF0ADB36E12F162DDFE93
SHA-512:	610B2210B8EC518928E7D762C68E9EDEE3E30D68BCEF6116BBB639FC6716EAC85CFD8FDAC0A4DD2F2A36E8213A5CB2B1D431E9026E3A7BDFC6E6B14FB6169B8A
Malicious:	false
Reputation:	low
Preview:	..<?x.m.l.v.e.r.s.i.o.n.="1..0".e.n.c.o.d.i.n.g.="U.T.F.-1.6"?.>.....<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<B.u.i.l.d.>.1.7.1.3.4.</B.u.i.l.d.>.....<P.r.o.d.u.c.t>.(0.x.3.0).;.W.i.n.d.o.w.s..1.0..P.r.o.</P.r.o.d.u.c.t>.....<E.d.i.t.i.o.n>.P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n.>.....<B.u.i.l.d.S.t.r.i.n.g>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.</B.u.i.l.d.S.t.r.i.n.g.>.....<R.e.v.i.s.i.o.n>.1.</R.e.v.i.s.i.o.n.>.....<F.l.a.v.o.r>.M.u.l.t.i.p.r.o.c.e.s.s.o.r..F.r.e.e.</F.l.a.v.o.r.>.....<A.r.c.h.i.t.e.c.t.u.r.e>.X.6.4.</A.r.c.h.i.t.e.c.t.u.r.e.>.....<L.C.I.D.>.1.0.3.3.</L.C.I.D.>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<P.i.d.>.4.6.0.4.</P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDE.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):	4.475132560980285
Encrypted:	false
SSDEEP:	48:cvlwSD8zsWJgtWl9EKWSC8Be8fm8M4JcdswNpFwA+q8/1NFP4SrSH1d:uITfsDrSNlJuNJ+NtDWH1d
MD5:	41DD7689AB47F12C55E21B43A8E52B56
SHA1:	608C7879B7F5CF81A03998F3C314BD3FD1489606
SHA-256:	137CAAC7EE6DE926423383024F01F76341D3ACC773A65B36FC833D553864C096
SHA-512:	137D9E0E64DE1CADA0EE87738C63540F66F0DFE7DF65199337FDC8595E1807EB7209ED222895F7927E962E74584FC0CDBAE35B2B32EDC9C68322FD7FB30E9CA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2"?>..<tlm>..<src>..<desc>..<mach>..<os>..<arg nm="vermaj" val="10" />..<arg nm="vermin" val="0" />..<arg nm="verbld" val="17134" />..<arg nm="vercsdbld" val="1" />..<arg nm="verqfe" val="1" />..<arg nm="csdbld" val="1" />..<arg nm="versp" val="0" />..<arg nm="arch" val="9" />..<arg nm="lcid" val="1033" />..<arg nm="geoid" val="244" />..<arg nm="sku" val="48" />..<arg nm="domain" val="0" />..<arg nm="prodsuite" val="256" />..<arg nm="ntprodtype" val="1" />..<arg nm="platid" val="2" />..<arg nm="tmsi" val="987781" />..<arg nm="osinsty" val="1" />..<arg nm="iever" val="11.1.17134.0-1 1.0.47" />..<arg nm="portos" val="0" />..<arg nm="ram" val="4096" />..

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ndows
Entropy (8bit):	7.510292716969832
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:	0f6f2d53_by_Libranalysis.dll
File size:	167424
MD5:	0f6f2d53b1f7eb793764036092bdec4b
SHA1:	8032adfdd6cef055e70e1816294f0b29042f9ee24
SHA256:	2cfd348c1d4dcc506269855b982b9cf97cf4e404a3b10df72112f7af2e35c41c
SHA512:	fb9d5af8a4d3b552b1ed6bf9495009894eddf4ae43327e62f658c1e5197a7bf0c1b142b124c6f6dc22f7c40e08ad384008008521d6081cf2f0f8ab1092cf85899
SSDEEP:	3072:yar6Ys6p54kfd0+APr0aYSbeO6aal8jeytFQT0pp2J:ks4p+ADxnSO6D2cOp
File Content Preview:	MZ.....@.....\.....!..L!Th is program cannot be run in DOS mode....\$.Xm.o...<...<...<U!<...<..B<r...<...<...<rQ!<...<...<...<3..<au.<...< szt<"...Rich...<.....

File Icon



Icon Hash:

74f0e4eccccde0e4

Static PE Info

General

Entrypoint:	0x10024b60
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:	0x609C7F8B [Thu May 13 01:23:23 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:	a5d8d3bddce161fe65c4f476bd18c6da

Entrypoint Preview

Instruction

[illegible]

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

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	0x23e31	0x23e00	False	0.753620426829	data	7.52981613282	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.749112215909	data	7.3747682631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x333c	0x1800	False	0.8125	MMDF mailbox	7.51564718747	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x5a1	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x268	0x400	False	0.5439453125	data	4.2612921869	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
CLUSAPI.dll	ClusterEnum
USER32.dll	TranslateMessage
KERNEL32.dll	LoadLibraryW, GetProfileSectionW, GetProfileSectionA, OpenSemaphoreW, CreateFileW, OutputDebugStringA, CloseHandle
ole32.dll	CreatePointerMoniker, CreateStreamOnHGlobal
ADVAPI32.dll	RegOverridePredefKey

DLL	Import
RASAPI32.dll	RasGetConnectionStatistics

Version Infos

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:50:44.005805969 CEST	57544	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:44.057369947 CEST	53	57544	8.8.8.8	192.168.2.3
May 13, 2021 06:50:44.893821955 CEST	55984	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:44.918414116 CEST	64185	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:44.947011948 CEST	53	55984	8.8.8.8	192.168.2.3
May 13, 2021 06:50:44.978004932 CEST	53	64185	8.8.8.8	192.168.2.3
May 13, 2021 06:50:45.658298969 CEST	65110	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:45.707046986 CEST	53	65110	8.8.8.8	192.168.2.3
May 13, 2021 06:50:46.497926950 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:46.546683073 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 06:50:47.302052021 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:47.350652933 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 06:50:48.239046097 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:48.291580915 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 06:50:49.304174900 CEST	60100	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:49.361140013 CEST	53	60100	8.8.8.8	192.168.2.3
May 13, 2021 06:50:50.215095997 CEST	53195	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:50.266612053 CEST	53	53195	8.8.8.8	192.168.2.3
May 13, 2021 06:50:51.054985046 CEST	50141	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:51.106137991 CEST	53	50141	8.8.8.8	192.168.2.3
May 13, 2021 06:50:51.922398090 CEST	53023	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:51.973964930 CEST	53	53023	8.8.8.8	192.168.2.3
May 13, 2021 06:50:52.748493910 CEST	49563	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:52.797317028 CEST	53	49563	8.8.8.8	192.168.2.3
May 13, 2021 06:50:53.783379078 CEST	51352	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:53.832123041 CEST	53	51352	8.8.8.8	192.168.2.3
May 13, 2021 06:50:54.748245955 CEST	59349	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:54.797141075 CEST	53	59349	8.8.8.8	192.168.2.3
May 13, 2021 06:50:55.539334059 CEST	57084	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:55.588237047 CEST	53	57084	8.8.8.8	192.168.2.3
May 13, 2021 06:50:56.905105114 CEST	58823	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:56.953881979 CEST	53	58823	8.8.8.8	192.168.2.3
May 13, 2021 06:50:57.718395948 CEST	57568	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:57.775496006 CEST	53	57568	8.8.8.8	192.168.2.3
May 13, 2021 06:50:58.523360968 CEST	50540	53	192.168.2.3	8.8.8.8
May 13, 2021 06:50:58.572166920 CEST	53	50540	8.8.8.8	192.168.2.3
May 13, 2021 06:51:19.036082983 CEST	54366	53	192.168.2.3	8.8.8.8
May 13, 2021 06:51:19.108906031 CEST	53	54366	8.8.8.8	192.168.2.3
May 13, 2021 06:51:22.249607086 CEST	53034	53	192.168.2.3	8.8.8.8
May 13, 2021 06:51:22.306509018 CEST	53	53034	8.8.8.8	192.168.2.3
May 13, 2021 06:51:28.438167095 CEST	57762	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:51:28.514791965 CEST	53	57762	8.8.8.8	192.168.2.3
May 13, 2021 06:51:33.860403061 CEST	55435	53	192.168.2.3	8.8.8.8
May 13, 2021 06:51:33.919058084 CEST	53	55435	8.8.8.8	192.168.2.3
May 13, 2021 06:52:07.497411013 CEST	50713	53	192.168.2.3	8.8.8.8
May 13, 2021 06:52:07.554785967 CEST	53	50713	8.8.8.8	192.168.2.3
May 13, 2021 06:52:15.522665024 CEST	56132	53	192.168.2.3	8.8.8.8
May 13, 2021 06:52:15.579762936 CEST	53	56132	8.8.8.8	192.168.2.3
May 13, 2021 06:52:32.738225937 CEST	58987	53	192.168.2.3	8.8.8.8
May 13, 2021 06:52:32.806385040 CEST	53	58987	8.8.8.8	192.168.2.3
May 13, 2021 06:52:44.629616022 CEST	56579	53	192.168.2.3	8.8.8.8
May 13, 2021 06:52:44.688116074 CEST	53	56579	8.8.8.8	192.168.2.3
May 13, 2021 06:52:47.173536062 CEST	60633	53	192.168.2.3	8.8.8.8
May 13, 2021 06:52:47.238276005 CEST	53	60633	8.8.8.8	192.168.2.3
May 13, 2021 06:53:17.787206888 CEST	61292	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:17.789727926 CEST	63619	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:17.845674992 CEST	53	61292	8.8.8.8	192.168.2.3
May 13, 2021 06:53:17.848439932 CEST	53	63619	8.8.8.8	192.168.2.3
May 13, 2021 06:53:40.835484028 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:40.895255089 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 06:53:41.546478987 CEST	61946	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:41.595206022 CEST	53	61946	8.8.8.8	192.168.2.3
May 13, 2021 06:53:42.201560020 CEST	64910	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:42.252028942 CEST	53	64910	8.8.8.8	192.168.2.3
May 13, 2021 06:53:42.719006062 CEST	52123	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:42.776463985 CEST	53	52123	8.8.8.8	192.168.2.3
May 13, 2021 06:53:43.347862959 CEST	56130	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:43.406532049 CEST	53	56130	8.8.8.8	192.168.2.3
May 13, 2021 06:53:43.971314907 CEST	56338	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:44.028544903 CEST	53	56338	8.8.8.8	192.168.2.3
May 13, 2021 06:53:44.523963928 CEST	59420	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:44.575532913 CEST	53	59420	8.8.8.8	192.168.2.3
May 13, 2021 06:53:45.410680056 CEST	58784	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:45.467849016 CEST	53	58784	8.8.8.8	192.168.2.3
May 13, 2021 06:53:46.276509047 CEST	63978	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:46.325265884 CEST	53	63978	8.8.8.8	192.168.2.3
May 13, 2021 06:53:46.804106951 CEST	62938	53	192.168.2.3	8.8.8.8
May 13, 2021 06:53:46.853013039 CEST	53	62938	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loadll32.exe PID: 4660 Parent PID: 5624

General

Start time:	06:50:50
Start date:	13/05/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\0f6f2d53_by_Libranalysis.dll'
Imagebase:	0xae0000
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: 5396 Parent PID: 4660

General

Start time:	06:50:51
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\0f6f2d53_by_Libranalysis.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

Analysis Process: rundll32.exe PID: 4604 Parent PID: 5396

General

Start time:	06:50:51
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe 'C:\Users\user\Desktop\0f6f2d53_by_Libranalysis.dll',#1
Imagebase:	0xb30000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.275435929.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 5672 Parent PID: 4604

General

Start time:	06:51:19
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4604 -s 764
Imagebase:	0x110000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	702B1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDE.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDE.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1710c1f71428debfe32e0ec35363e2ed6ae718d_82810a17_1612a3b8	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1710c1f71428debfe32e0ec35363e2ed6ae718d_82810a17_1612a3b8\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDE.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.tmp.dmp	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDE.tmp.xml	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERED2C.tmp.csv	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERED4C.tmp.txt	success or wait	1	702A4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 d9 2e 9d 60 a4 05 12 00 00 00 00 00	MDMP.....`.....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.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 08 20 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 fc 11 00 00 bb 2e 9d 60 07 00 00 00 10 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	U.....B..... ..GenuineIntelW.....T...`.....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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 c2 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 30 2a 02 00 00 00 00 00 00 a6 02 00 00 00 00 34 57 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 76 e8 00 00 00 00 00 00 70 5e 03 00 00 00 00 00 c3 8c 02 00 00 00 00 00 ff ff ff ff 00 00 00 ef c4 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 a6 d6 21 00 00 00 00	..Ht....0...U..s@...%.....B.....B?.....#..... ..@A.....Zb.....0*..... 4W.....v.....p^! @.....!....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.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.....l.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9AAF.tmp.dmp	unknown	108	03 00 00 00 f4 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 fc 07 00 00 05 00 00 00 64 01 00 00 a4 36 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 be cb 00 00 15 00 00 00 ec 01 00 00 84 1d 00 00 16 00 00 00 98 00 00 00 70 1f 00 00	d. ...6.....T.....8..... ...T.....`.....p...	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?.x.m.l..v.e.r.s.i.o.n.=." 1...0". .e.n.c.o.d.i.n.g.=." U.T.F.-.1.6".?>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<.W.E.R.R.e.p.o.r.t.M.e.t.a d.a.t.a.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.l.n.f.o.r m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.W.i.n.d.o.w.s.N.T.V.e.r.s. i.o.n.>.1.0...0. </.W.i.n.d.o.w. s.N.T.V.e.r.s.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<.B.u.i.l.d.>.1.7.1.3.4.</.B. u.i.l.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<.P.r.o.d.u.c.t>.(0.x.3.0). : .W.i.n.d.o.w.s. .1.0. .P.r. o.<./P.r.o.d.u.c.t>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<.E.d.i.t.i.o.n>.P.r.o.f.e.s. s.i.o.n.a.l.<./E.d.i.t.i.o.n>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<.B.u.i.l.d.S.t.r.i.n.g>.1.7. 1.3.4...1...a.m.d.6.4.f.r.e... r.s.4._r.e.l.e.a.s.e...1.8.0. 4.1.0.-1.8.0.4.<./B.u.i.l.d. S.t.r.i.n.g>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<.R.e.v.i.s.i.o.n>.1.<./R.e. v.i.s.i.o.n>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<.F.l.a.v.o.r>.M.u.l.t.i.p.r. o.c.e.s.s.o.r. .F.r.e.e.<./F. l.a.v.o.r>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./L.C.I.D.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 36 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.6.0.4.<./P.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.I.I.3.2...e.x.e.<./I.m.a.g.e.N.a.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 39 00 38 00 30 00 32 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.>.2.9.8.0.2.<./U.p.t.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<.W.o.w.6.4.g.u.e.s.t.=."3.3.2".h.o.s.t.=."3.4.4.0.4".>.1.<./W.o.w.6.4.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.l.p.t.E.n.a.b.l.e.d.>.0.<./l.p.t.E.n.a.b.l.e.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 33 00 34 00 38 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.3.4.8.1.6.0.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 38 00 33 00 33 00 39 00 39 00 36 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.8.3.3.9.9.6.8.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.4.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 36 00 35 00 31 00 35 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.>.9.2.6.5.1.5.2.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 36 00 35 00 31 00 35 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.>.9.2.6.5.1.5.2.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.4.1.6.<./Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.1.8.4.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 31 00 31 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.I.U.s.a.g.e>.3.1.1.1.2.<./Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.3.0.8.4.0.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 35 00 32 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e>.6.0.2.5.2.1.6.<./P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 33 00 33 00 34 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e>.6.0.3.3.4.0.8.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 30 00 32 00 35 00 32 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e>.6.0.2.5.2.1.6.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.V.m.l.n.f.o.r.m.a.t.i.o.n>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<.P.a.r.e.n.t.P.r.o.c.e.s.s>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.P.r.o.c.e.s.s.l.n.f.o.r.m.a.t.i.o.n>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 33 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d>.5.3.9.6.<./P.i.d>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.0.0.0.0.0.0.0.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 31 00 32 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<U.p.t.i.m.e>.3.0.1.2.2.<./U.p.t.i.m.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<W.o.w.6.4.g.u.e.s.t.="3.3.2".h.o.s.t.="3.4.4.0.4".>.1.<./W.o.w.6.4>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<I.p.t.E.n.a.b.l.e.d>.0.<./I.p.t.E.n.a.b.l.e.d>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.7.4.0.5.4.4.0.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 33 00 34 00 34 00 30 00 35 00 31 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.>.5.3.4.4.0.5.1.2.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 31 00 37 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.>.1.1.1.7.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 31 00 35 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.1.5.0.7.2.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 37 00 30 00 32 00 37 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.0.2.7.8.4.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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	<Quota.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.4.0.9.6.0.<./Quota.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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	<Quota.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.3.3.2.1.6.<./Quota.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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	<Quota.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.<./Quota.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<Quota.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.5.2.2.4.<./Quota.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 33 00 34 00 31 00 31 00 39 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.4.1.1.9.6.8.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 36 00 33 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.6.3.5.2.0.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 33 00 34 00 31 00 31 00 39 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.3.4.1.1.9.6.8.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.V.m.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<E.v.e.n.t.T.y.p.e.>.A.P.P.C.R.A.S.H.<./E.v.e.n.t.T.y.p.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<P.a.r.a.m.e.t.e.r.0>.r.u.n.d.l.l.3.2...e.x.e.<./P.a.r.a.m.e.t.e.r.0>.	success or wait	8	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./P.r.o.b.l.e.m.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...2.5.6...4.8.<./P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<./D.y.n.a.m.i.c.S.i.g.n.a.t.u.r.e.s.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<.M.I.D.>.A.2.A.B.5.2.6.A.-.D.3.8.D.-.4.F.C.9.-.8.B.A.0.-.E.3.4.B.8.D.6.3.5.4.E.8.<./M.I.D.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 63 00 65 00 62 00 74 00 62 00 77 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.>.c.e.b.t.b.w.,.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 63 00 65 00 62 00 74 00 62 00 77 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>.c.e.b.t.b.w.7.,.1.</.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.</.B.I.O.S.V.e.r.s.i.o.n>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 39 00 33 00 39 00 33 00 35 00 35 00 33 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>.1.5.6.9.3.9.3.5.5.3.</.O.S.I.n.s.t.a.l.l.D.a.t.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.T.i.m.e>.2.0.1.9.-.0.6.-.2.7.T.1.4.:.4.9.:2.1.Z.</.O.S.I.n.s.t.a.l.l.T.i.m.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.0.<./U.E.F.I.S.e.c.u.r.e.B.o.o.t.E.n.a.b.l.e.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<./S.e.c.u.r.e.B.o.o.t.S.t.a.t.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<.I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<F.l.a.g.s>.0.0.0.0.0.0.0.0<./F.l.a.g.s.>.	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<./I.n.t.e.g.r.a.t.o.r.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 35 00 31 00 3a 00 32 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.= ".2.0. 2.1.-0.5.-1.3.T.1.3.:5.1:.. 2.1.Z.">.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.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 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 36 00 30 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 37 00 34 00 32 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 37 00 34 00 32 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 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.l.d.= ".3.4.3". .P.I.D.= ".4.6.0.4". .U.p.t.i.m.e.M.S.= ".2.7.4.2.1". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".2.7.4.2.1". .S.u.s.p.e.n.d.e.d.M.S.= ".0". .H.a.n.g.C.o.u.n.t.= ".0". .G.h.o.s.t.C.o.u.n.t.= ".0". .C.r.a.s.h.e.d	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./P.r.o.c.e.s.s.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	<./P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 61 00 33 00 35 00 65 00 33 00 66 00 38 00 2d 00 61 00 30 00 62 00 33 00 2d 00 34 00 66 00 65 00 38 00 2d 00 38 00 34 00 62 00 61 00 2d 00 35 00 38 00 65 00 35 00 30 00 38 00 32 00 34 00 66 00 39 00 61 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.9.a.3.5.e.3.f.8.-.a.0.b.3.-.4.f.e.8.-.8.4.b.a.-.5.8.e.5.0.8.2.4.f.9.a.7.<./G.u.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 35 00 31 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.3.:.5.1.:.2.1.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./R.e.p.o.r.t.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9D11.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<./W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9DDE.tmp.xml	unknown	4663	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>.. ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1710c1f71428debfe32e0ec35363e2ed6ae718d_82810a17_1612a3b8\Report.wer	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1710c1f71428debfe32e0ec35363e2ed6ae718d_82810a17_1612a3b8\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	182	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_1710c1f71428debfe32e0ec35363e2ed6ae718d_82810a17_1612a3b8\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 35 00 37 00 38 00 30 00 37 00 34 00 38 00 33 00 37 00	M.e.t.a.d.a.t.a.H.a.s.h.=.5. 7.8.0.7.4.8.3.7.	success or wait	1	702A497A	unknown

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRYA\{9b9330db-f1be-1a71-78ab-951a4de778e4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRYA\{9b9330db-f1be-1a71-78ab-951a4de778e4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRYA\{9b9330db-f1be-1a71-78ab-951a4de778e4}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	success or wait	1	702C36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	702C1FB2	RegCreateKeyExW
\REGISTRYA\{9b9330db-f1be-1a71-78ab-951a4de778e4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702A43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{9b9330db-f1be-1a71-78ab-951a4de778e4}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	ProgramId	unicode	0000f519fec486de87ed73cb92d3cac802400000000	success or wait	1	702C36BF	unknown
\REGISTRYA\{9b9330db-f1be-1a71-78ab-951a4de778e4}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	702C36BF	unknown

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