

JoeSandbox Cloud BASIC



ID: 413035

Sample Name:

c2b6efb1_by_Libranalysis.dll

Cookbook: default.jbs

Time: 06:48:10

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report c2b6efb1_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
URLs from Memory and Binaries	8
Contacted IPs	8
Public	8
Private	8
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	10
ASN	11
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	13
General	13
File Icon	14
Static PE Info	14
General	14
Entrypoint Preview	14
Rich Headers	15
Data Directories	15
Sections	15
Resources	16
Imports	16
Version Infos	16

Network Behavior	16
UDP Packets	16
Code Manipulations	18
Statistics	18
Behavior	18
System Behavior	18
Analysis Process: loaddll32.exe PID: 5876 Parent PID: 5748	18
General	18
File Activities	18
Analysis Process: cmd.exe PID: 1656 Parent PID: 5876	18
General	18
File Activities	19
Analysis Process: rundll32.exe PID: 1892 Parent PID: 1656	19
General	19
Analysis Process: WerFault.exe PID: 6964 Parent PID: 1892	19
General	19
File Activities	19
File Created	19
File Deleted	20
File Written	20
Registry Activities	42
Key Created	42
Key Value Created	42
Disassembly	43
Code Analysis	43

Analysis Report c2b6efb1_by_Libranalysis.dll

Overview

General Information

Sample Name:

c2b6efb1_by_Libranalysis.dll

Analysis ID:

413035

MD5:

c2b6efb1b15eab8.

SHA1:

fab251bf2316a77..

SHA256:

2626744dae6404..

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...

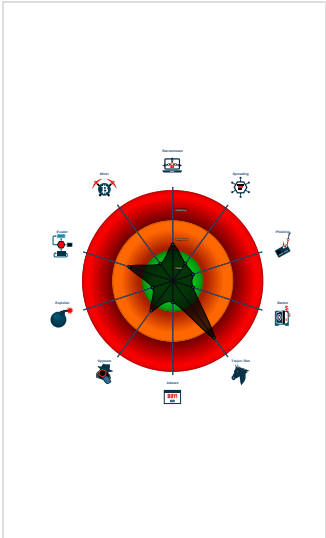
Detected potential crypto function

IP address seen in connection with o...

Internet Provider seen in connection...

Monitors certain registry keys / valu...

Classification



Startup

System is w10x64

loadll32.exe (PID: 5876 cmdline: loadll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 1656 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 1892 cmdline: rundll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 6964 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 1892 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

cleanup

Malware Configuration

Threatname: Dridex

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.336732319.0000000010001000.0000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Copyright Joe Security LLC 2021

Page 4 of 43

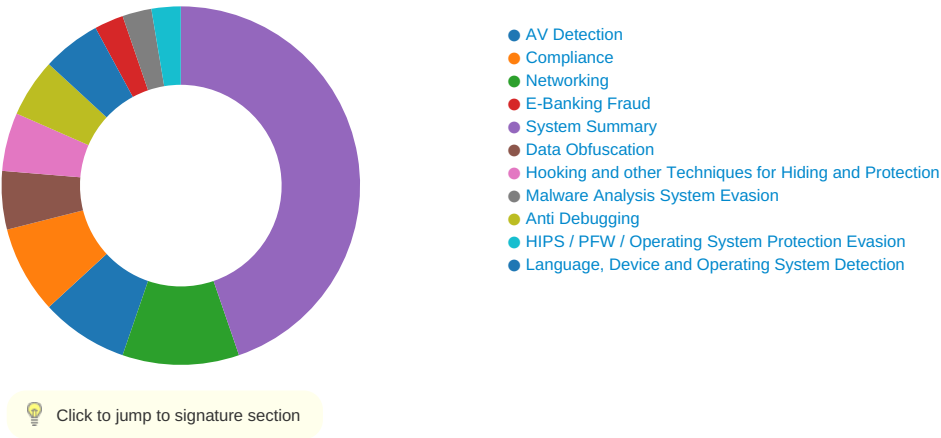
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

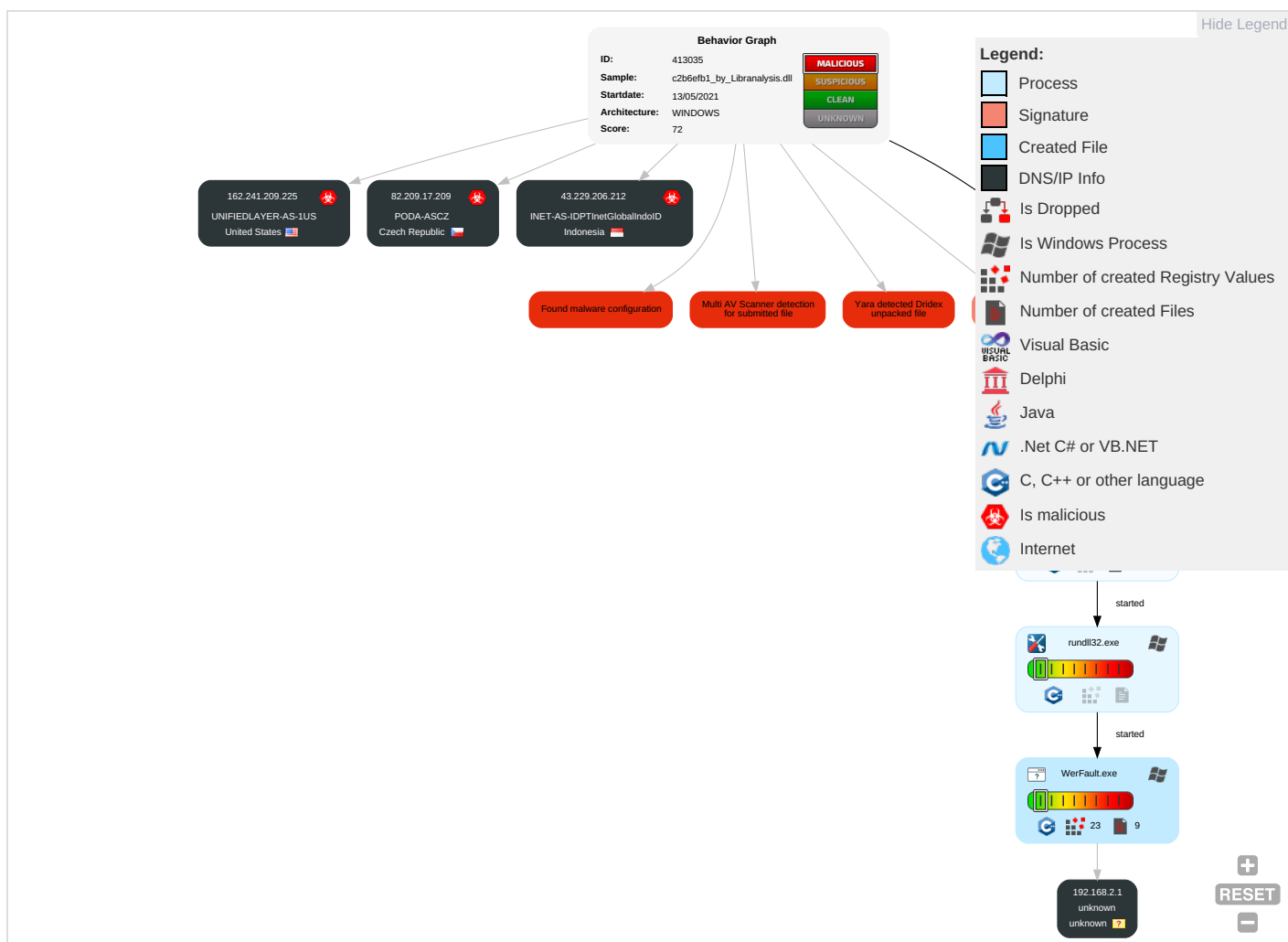
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

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

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

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.
Copyright Joe Security LLC 2021



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
c2b6efb1_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
c2b6efb1_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.2de0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	

Domains and IPs

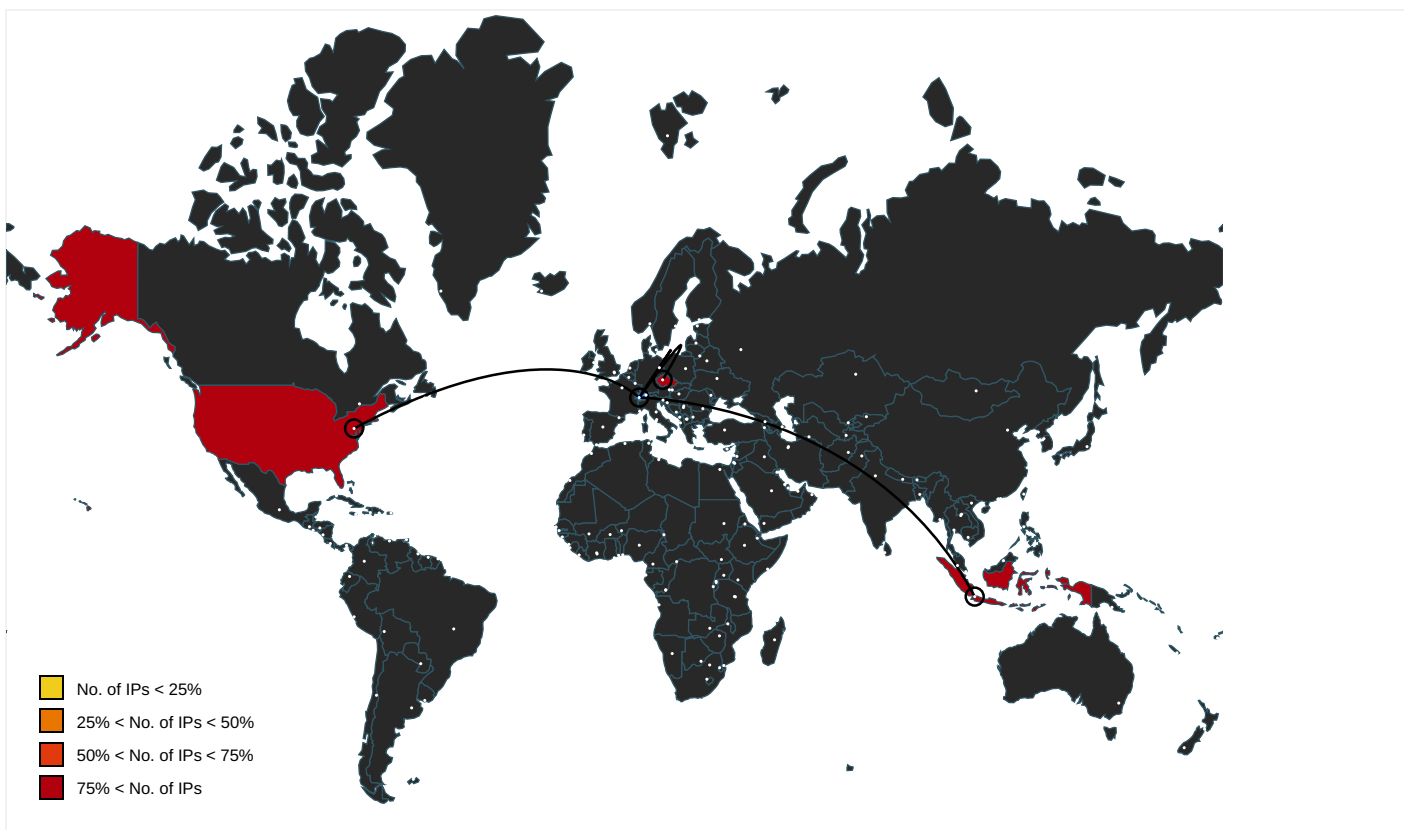
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.microsoft	WerFault.exe, 0000000F.00000000 3.331018665.0000000004FCD000.0 00000004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413035
Start date:	13.05.2021
Start time:	06:48:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c2b6efb1_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:	35
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@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 94.4% (good quality ratio 86.6%) • Quality average: 72.2% • Quality standard deviation: 32%
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	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	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	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	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	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	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	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
	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
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	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
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	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

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	
Preview:	MDMP.....s.`.....U.....B.....x.....GenuineIntelW.....T.....d..M.`.....0.=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4..1...x.8.6.f.r.e...r.s.4_..r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,1.0...0..1.7.1.3.4..1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8292
Entropy (8bit):	3.697409060736895
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi/F6336YvL66egmfTnVSZCpr889bhEsfwLm:RrlsNi96n6YT66egmfTVSlh3fB
MD5:	5CAE14732630676DCC24340983E81733
SHA1:	781806872C49CFB2991C09E433DD55D18E497E79
SHA-256:	5BC9F9C959F49600110B9A791A09FEFB8B6A3EA66D7B47D5B62883BCD6DC10F5
SHA-512:	FAAEB6FEC452DC4E9779B3EF61328E30E3B30430FDB06705C5276958073F87D7C0AFE92B4E1DD2F157FAFB4709DD439236AC9AC4DEBC69CDEFF71A49BA4D7.31
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>.(0x3.0);. .W.i.n.d.o.w.s. .1.0. .P.r.o. </P.r.o.d.u.c.t>.....<E.d.i.t.i.o.n>P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n.>.....<B.u.i.l.d.S.t.r.i.n.g>1.7.1.3.4..1...a.m.d.6.4.f.r.e...r.s.4_..r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4. </B.u.i.l.d.S.t.r.i.n.g>.....<R.e.v.i.s.i.o.n>1</R.e.v.i.s.i.o.n>.....<F.l.a.v.o.r>M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</F.l.a.v.o.r>.....<A.r.c.h.i.t.e.c.t.u.r.e>X.6.4.</ A.r.c.h.i.t.e.c.t.u.r.e>.....<L.C.I.D>1.0.3.3.</L.C.I.D>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<P.i.d>1.8.9.2.</P.i. d>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER80F6.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):	4.476322018756217
Encrypted:	false
SSDEEP:	48:cvlwSD8zstJgtWI97JWSC8Bg8fm8M4JCdsLNrFea+q8/ufNF54SrSpd:ulTfH4SSNPJ9NQaNNnDWPd
MD5:	4C3573F2F575F6446E42506D7245B261
SHA1:	126C7F8391DAF0169A77CB819EBFF411F4AEE8DD
SHA-256:	D8928C9FBC9B396BD07E9F709341E9FE2A2AE3F6168B790040D664DD38FC7983
SHA-512:	B1D3B6694AE0BB6298F6E5D421A3E48E47B3EAC59B60529EEC7AF42C6724FD5C67D6C21ABBD88534B559A657A6851539452419D98184E0EFD7676224DACA5E4C
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="987780" />.. <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):	7.513878784862757
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:	c2b6efb1_by_Libranalysis.dll
File size:	167424
MD5:	c2b6efb1b15eab83bcec9afd875fbb34

General	
SHA1:	fab251bf2316a77c53f3b92ad016ed9697f4f14a
SHA256:	2626744dae64045e445cbab9a2a225827d362ef6a0c20ea56b67dcec779857e
SHA512:	632e3cb1ff7220b5ecc5800ecef4d6ebd69ff7a21d040e76a0a5dce9f06103b98bc3e60b05a34bf2e240ec91b89f028a0436f7b3760e3cb291327d123c5dfb66
SSDEEP:	3072:89F/oNrQb4xVubbxP/NTccbsFvCeLmXH57V30e8Pj:89F6rQXvFczvYpQP
File Content Preview:	MZ.....@.....\.....!..L!Th is program cannot be run in DOS mode...\$.....Xm.o...< ...<...<U!<...<.B<r...<...<...<rQ!<...<...<...<3..<au.<...< szt<".<Rich...<.....

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x10024cc0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	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:	88962f6760ea005847fb88b87e8ce1fd

Entrypoint Preview

Instruction	
mov eax, 00000000h	
cmpss xmm1, xmm2, 03h	
mov edx, 00000000h	
mov edx, 00000000h	
mov edx, 00000000h	
mov edx, 00000000h	
mov edx, 00000000h	
mov edx, 00000000h	
mov edx, 00000000h	
cmpss xmm1, xmm2, 03h	
cmp eax, 02h	
mov eax, ebp	
mov dword ptr [10029734h], eax	
mov eax, ebx	
mov dword ptr [10029730h], eax	
mov eax, esi	
mov dword ptr [10029728h], eax	
jne 00007F0178BF8516h	
mov eax, 00000000h	
mov eax, 00000000h	
mov eax, 00000000h	
mov eax, 00000000h	

Instruction
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
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	0x23dfe	0x23e00	False	0.756362968206	data	7.53078515147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x389c	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x3a0	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x2d000	0x26c	0x400	False	0.548828125	data	4.2946697642	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Version Infos

Description	Data
LegalCopyright	Copyright 2018
InternalName	x2otfb
FileVersion	7.2.5422.00
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 06:48:54.927076101 CEST	62452	53	192.168.2.7	8.8.8.8
May 13, 2021 06:48:54.984257936 CEST	53	62452	8.8.8.8	192.168.2.7
May 13, 2021 06:48:55.171713114 CEST	57820	53	192.168.2.7	8.8.8.8
May 13, 2021 06:48:55.252832890 CEST	53	57820	8.8.8.8	192.168.2.7
May 13, 2021 06:48:55.280885935 CEST	50848	53	192.168.2.7	8.8.8.8
May 13, 2021 06:48:55.329447031 CEST	53	50848	8.8.8.8	192.168.2.7
May 13, 2021 06:48:56.185048103 CEST	61242	53	192.168.2.7	8.8.8.8
May 13, 2021 06:48:56.236711025 CEST	53	61242	8.8.8.8	192.168.2.7
May 13, 2021 06:48:58.229304075 CEST	58562	53	192.168.2.7	8.8.8.8
May 13, 2021 06:48:58.281188965 CEST	53	58562	8.8.8.8	192.168.2.7
May 13, 2021 06:48:58.386735916 CEST	56590	53	192.168.2.7	8.8.8.8
May 13, 2021 06:48:58.445003033 CEST	53	56590	8.8.8.8	192.168.2.7
May 13, 2021 06:49:05.846982956 CEST	60501	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:05.895843983 CEST	53	60501	8.8.8.8	192.168.2.7
May 13, 2021 06:49:07.385124922 CEST	53775	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:07.433958054 CEST	53	53775	8.8.8.8	192.168.2.7
May 13, 2021 06:49:08.334858894 CEST	51837	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:08.386565924 CEST	53	51837	8.8.8.8	192.168.2.7
May 13, 2021 06:49:09.291532040 CEST	55411	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:09.340286970 CEST	53	55411	8.8.8.8	192.168.2.7
May 13, 2021 06:49:10.527621031 CEST	63668	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:49:10.584943056 CEST	53	63668	8.8.8.8	192.168.2.7
May 13, 2021 06:49:14.258850098 CEST	54640	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:14.312367916 CEST	53	54640	8.8.8.8	192.168.2.7
May 13, 2021 06:49:20.345279932 CEST	58739	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:20.404223919 CEST	53	58739	8.8.8.8	192.168.2.7
May 13, 2021 06:49:21.145508051 CEST	60338	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:21.202756882 CEST	53	60338	8.8.8.8	192.168.2.7
May 13, 2021 06:49:34.299740076 CEST	58717	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:34.348427057 CEST	53	58717	8.8.8.8	192.168.2.7
May 13, 2021 06:49:37.242156982 CEST	59762	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:37.291122913 CEST	53	59762	8.8.8.8	192.168.2.7
May 13, 2021 06:49:39.019931078 CEST	54329	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:39.069077969 CEST	53	54329	8.8.8.8	192.168.2.7
May 13, 2021 06:49:40.507560968 CEST	58052	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:40.559079885 CEST	53	58052	8.8.8.8	192.168.2.7
May 13, 2021 06:49:41.841483116 CEST	54008	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:41.890173912 CEST	53	54008	8.8.8.8	192.168.2.7
May 13, 2021 06:49:42.654915094 CEST	59451	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:42.703866005 CEST	53	59451	8.8.8.8	192.168.2.7
May 13, 2021 06:49:43.804554939 CEST	52914	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:43.853194952 CEST	53	52914	8.8.8.8	192.168.2.7
May 13, 2021 06:49:44.658557892 CEST	64569	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:44.707227945 CEST	53	64569	8.8.8.8	192.168.2.7
May 13, 2021 06:49:45.483679056 CEST	52816	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:45.533509016 CEST	53	52816	8.8.8.8	192.168.2.7
May 13, 2021 06:49:46.351516008 CEST	50781	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:46.403043985 CEST	53	50781	8.8.8.8	192.168.2.7
May 13, 2021 06:49:46.855834007 CEST	54230	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:46.928221941 CEST	53	54230	8.8.8.8	192.168.2.7
May 13, 2021 06:49:47.202011108 CEST	54911	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:47.252136946 CEST	53	54911	8.8.8.8	192.168.2.7
May 13, 2021 06:49:47.340672016 CEST	49958	53	192.168.2.7	8.8.8.8
May 13, 2021 06:49:47.389424086 CEST	53	49958	8.8.8.8	192.168.2.7
May 13, 2021 06:50:05.727495909 CEST	50860	53	192.168.2.7	8.8.8.8
May 13, 2021 06:50:05.786201954 CEST	53	50860	8.8.8.8	192.168.2.7
May 13, 2021 06:50:37.219923973 CEST	50452	53	192.168.2.7	8.8.8.8
May 13, 2021 06:50:37.285640955 CEST	53	50452	8.8.8.8	192.168.2.7
May 13, 2021 06:50:44.780266047 CEST	59730	53	192.168.2.7	8.8.8.8
May 13, 2021 06:50:44.839905977 CEST	53	59730	8.8.8.8	192.168.2.7
May 13, 2021 06:51:00.224630117 CEST	59310	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:00.362534046 CEST	53	59310	8.8.8.8	192.168.2.7
May 13, 2021 06:51:01.027856112 CEST	51919	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:01.085012913 CEST	53	51919	8.8.8.8	192.168.2.7
May 13, 2021 06:51:01.692533970 CEST	64296	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:01.752146006 CEST	53	64296	8.8.8.8	192.168.2.7
May 13, 2021 06:51:02.190048933 CEST	56680	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:02.229018927 CEST	58820	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:02.255911112 CEST	53	56680	8.8.8.8	192.168.2.7
May 13, 2021 06:51:02.282416105 CEST	53	58820	8.8.8.8	192.168.2.7
May 13, 2021 06:51:02.876241922 CEST	60983	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:03.015160084 CEST	53	60983	8.8.8.8	192.168.2.7
May 13, 2021 06:51:03.628478050 CEST	49247	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:03.685518980 CEST	53	49247	8.8.8.8	192.168.2.7
May 13, 2021 06:51:04.359869003 CEST	52286	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:04.418692112 CEST	53	52286	8.8.8.8	192.168.2.7
May 13, 2021 06:51:05.716070890 CEST	56064	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:05.773072004 CEST	53	56064	8.8.8.8	192.168.2.7
May 13, 2021 06:51:06.620724916 CEST	63744	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:06.680651903 CEST	53	63744	8.8.8.8	192.168.2.7
May 13, 2021 06:51:07.296525955 CEST	61457	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:07.345268011 CEST	53	61457	8.8.8.8	192.168.2.7
May 13, 2021 06:51:17.404393911 CEST	58367	53	192.168.2.7	8.8.8.8
May 13, 2021 06:51:17.464802980 CEST	53	58367	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



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

Click to jump to process

System Behavior

Analysis Process: loadll32.exe PID: 5876 Parent PID: 5748

General

Start time:	06:49:00
Start date:	13/05/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll'
Imagebase:	0x11f0000
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: 1656 Parent PID: 5876

General

Start time:	06:49:00
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\c2b6efb1_by_Libranalysis.dll',#1
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

Analysis Process: rundll32.exe PID: 1892 Parent PID: 1656

General

Start time:	06:49:01
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\c2b6efb1_by_Libranalysis.dll',#1
Imagebase:	0xa00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.336732319.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6964 Parent PID: 1892

General

Start time:	06:49:33
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 1892 -s 764
Imagebase:	0x9b0000
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
-----------	--------	------------	---------	------------	-------	----------------	--------

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	6CD61717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80F6.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80F6.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1b7d9d17	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1b7d9d17\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6CD5497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80F6.tmp	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	success or wait	1	6CD54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	success or wait	1	6CD54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80F6.tmp.xml	success or wait	1	6CD54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8104.tmp.csv	success or wait	1	6CD54BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8710.tmp.txt	success or wait	1	6CD54BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 73 2e 9d 60 a4 05 12 00 00 00 00 00	MDMP.....S..`.....	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	unknown	168	a0 17 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 ca 30 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 19 06 00 02 00 cc 02 00 00 4c 25 00 00	0....L%..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	unknown	20	0c 00 00 00 18 08 28 03 00 00 00 00 04 00 00 00 74 2e 00 00	(.....t..	success or wait	12	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	unknown	4	74 68 65 6d	them	success or wait	11	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	unknown	952	bc b1 30 77 d6 c9 2e 77 64 02 00 00 aa aa aa aa 10 00 00 00 dc fc b3 04 a8 fd b3 04 aa aa aa aa 40 c7 2e 77 40 c7 2e 77 a8 07 04 03 00 00 fa 02 00 00 fa 02 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 00 fa 02 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 78 19 05 03 00 00 00 00 00 00 00 00 48 09 04 03 00 40 f9 02 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a8 07 04 03 00 00 00 00 aa aa aa aa aa aa aa aa 54 42 f9 02 54 42 f9 02 e0 07 04 03 e0 07 04 03 00 00 00 00 aa aa aa aa a8 07 04 03 00	..0w...wd..... ..@..w@..w.....d..d.....X....H...@.....TB..TB	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	unknown	4	02 00 00 00		success or wait	2	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7607.tmp.dmp	unknown	108	03 00 00 00 64 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 6c 07 00 00 05 00 00 00 c4 00 00 00 b0 2d 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 ca 7b 00 00 15 00 00 00 ec 01 00 00 f4 1c 00 00 16 00 00 00 98 00 00 00 e0 1e 00 00	d.....l.....-T.....8..... ...T.....`...{.....	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r. m.a.t.i.o.n>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	<.Architecture>.X.64.<.Architecture>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	<.LCID>.1.0.3.3.<.LCID>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	<.OS.Version.Information>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	<.Process.Information>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 38 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.Pid>.1.8.9.2.<.Pid>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	<.ImageName>.run.dll.3.2...exe.<.ImageName>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	<.CommandLineSignature>.0.0.0.0.0.0.0.<.CommandLineSignature>.	success or wait	1	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 38 00 34 00 38 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.8.4.8.6.<./U.p.t.i.m.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 36 00 37 00 37 00 35 00 32 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.6.7.7.5.2.9.6.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 36 00 37 00 36 00 37 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.6.7.6.7.1.0.4.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.3.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 31 00 37 00 39 00 31 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.7.9.1.3.6.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 31 00 37 00 39 00 31 00 33 00 36 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.>.9.1.7.9.1.3.6.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.6.4.0.<./Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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.l.U.s.a.g.e>.1.8.4.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 32 00 39 00 38 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.2.9.8.4.8.<./Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.2.9.5.7.6.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 30 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e>.5.7.0.9.8.2.4.<./P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 31 00 38 00 30 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.7.1.8.0.1.6. <./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 30 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.7.0.9.8.2.4.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 36 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.1.6.5.6.<./P.i.d.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.c.m.d...e.x.e. <./I.m.a.g.e.N.a.m.e.>.	success or wait	1	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.0.0.0.0.0.0.0.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 38 00 38 00 36 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>.3.8.8.6.2.<./U.p.t.i.m.e>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 31 00 32 00 39 00 37 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.2.1.2.9.7.9.2.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.4. <./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 33 00 31 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.3.1.4.5.6. <./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 39 00 34 00 35 00 39 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.9.4.5.9.2. <./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.0.9.6.0.<./Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.6.3.2.<./Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.9.5.2.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 38 00 32 00 31 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.4.8.2.1.7.6.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 39 00 32 00 31 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.9.2.1.9.2.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 34 00 38 00 32 00 31 00 37 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.>.2.4.8.2.1.7.6.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 6f 00 64 00 78 00 75 00 79 00 75 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 65 00 72 00 3e 00	<S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.o.d.x.u.y.u.,.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 6f 00 64 00 78 00 75 00 79 00 75 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>.o.d.x.u.y.u.7.,.1.</.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 37 00 36 00 32 00 39 00 38 00 32 00 32 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>.1.5.6.7.6.2.9.8.2.2.</.O.S.I.n.s.t.a.l.l.D.a.t.e>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.<./F.l.a.g.s.>.	success or wait	3	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 34 00 39 00 3a 00 33 00 39 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.:4.9.: 3.9.Z.">.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 34 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 38 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 30 00 38 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 30 00 38 00 31 00 32 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 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<P.r.o.c.e.s.s. .A.s.I.d.="3.4.1". .P.I.D.="1.8.9.2". .U.p.t.i.m.e.M.S.="3.0.8.1.2". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.="3.0.8.1.2". .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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.i.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 37 00 35 00 30 00 62 00 30 00 38 00 62 00 2d 00 30 00 35 00 35 00 38 00 2d 00 34 00 37 00 37 00 37 00 2d 00 61 00 32 00 35 00 37 00 2d 00 62 00 38 00 37 00 61 00 66 00 61 00 35 00 36 00 32 00 33 00 31 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.5.7.5.0.b.0.8.b.-.0.5.5.8.-.4.7.7.7.-.a.2.5.7.-.b.8.7.a.f.a.5.6.2.3.1.d.<./G.u.i.d.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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 34 00 39 00 3a 00 33 00 39 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.:4.9.:3.9.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./R.e.p.o.r.t.i.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7ED2.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	6CD5497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80F6.tmp.xml	unknown	4663	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>.<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" >.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1b7d9d17\Report.wer	unknown	2	ff fe	..	success or wait	1	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1b7d9d17\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	181	6CD5497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_ceab9952f15a603fe8bb7fca6d086e06c93d7dd_82810a17_1b7d9d17\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 35 00 32 00 30 00 30 00 30 00 33 00 33 00 33 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.- .1.5.2.0.0.0.3.3.3.3.	success or wait	1	6CD5497A	unknown

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRYA\{c51a270d-8414-5c63-5e70-e6376f5ff1ce}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CD736BF	unknown
\REGISTRYA\{c51a270d-8414-5c63-5e70-e6376f5ff1ce}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CD736BF	unknown
\REGISTRYA\{c51a270d-8414-5c63-5e70-e6376f5ff1ce}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6CD736BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6CD71FB2	RegCreateKeyExW
\REGISTRYA\{c51a270d-8414-5c63-5e70-e6376f5ff1ce}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6CD543D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{c51a270d-8414-5c63-5e70-e6376f5ff1ce}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519fec486de87ed73cb92d3cac802400000000	success or wait	1	6CD736BF	unknown
\REGISTRYA\{c51a270d-8414-5c63-5e70-e6376f5ff1ce}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6CD736BF	unknown

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