ID: 413066
Sample Name:
1cc57949_by_Libranalysis.dll
Cookbook: default.jbs
Time: 07:32:51
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

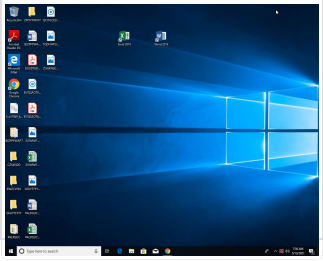
Analysis Report 1cc57949_by_Libranalysis.dll

Overview

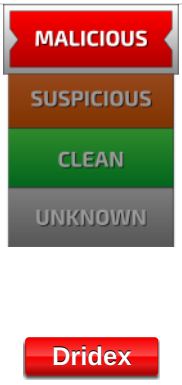
General Information

Sample Name:	1cc57949_by_Libranalysis.dll
Analysis ID:	413066
MD5:	1cc57949b45974..
SHA1:	0dceb93b98a9bc..
SHA256:	814739bdf67c1f2..
Infos:	

Most interesting Screenshot:



Detection

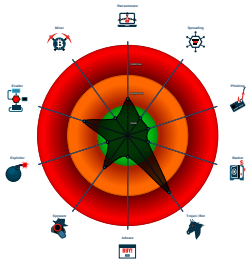


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function
- IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 2168 cmdline: loaddll32.exe 'C:\Users\user\Desktop\1cc57949_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6064 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\1cc57949_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5992 cmdline: rundll32.exe 'C:\Users\user\Desktop\1cc57949_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 4120 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5992 -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": [
    "16dkGStOzdHgjuCciXGdSX7UrHWfYSUG8wEUtKNgzHrWMfTGafJbC",
    "39t3NdDhurvpltFNCpvA5goSylkxjIBtIwWPTv1DPbNEcuIekQC7O"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.301331659.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

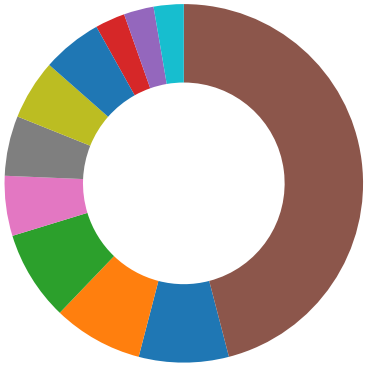
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

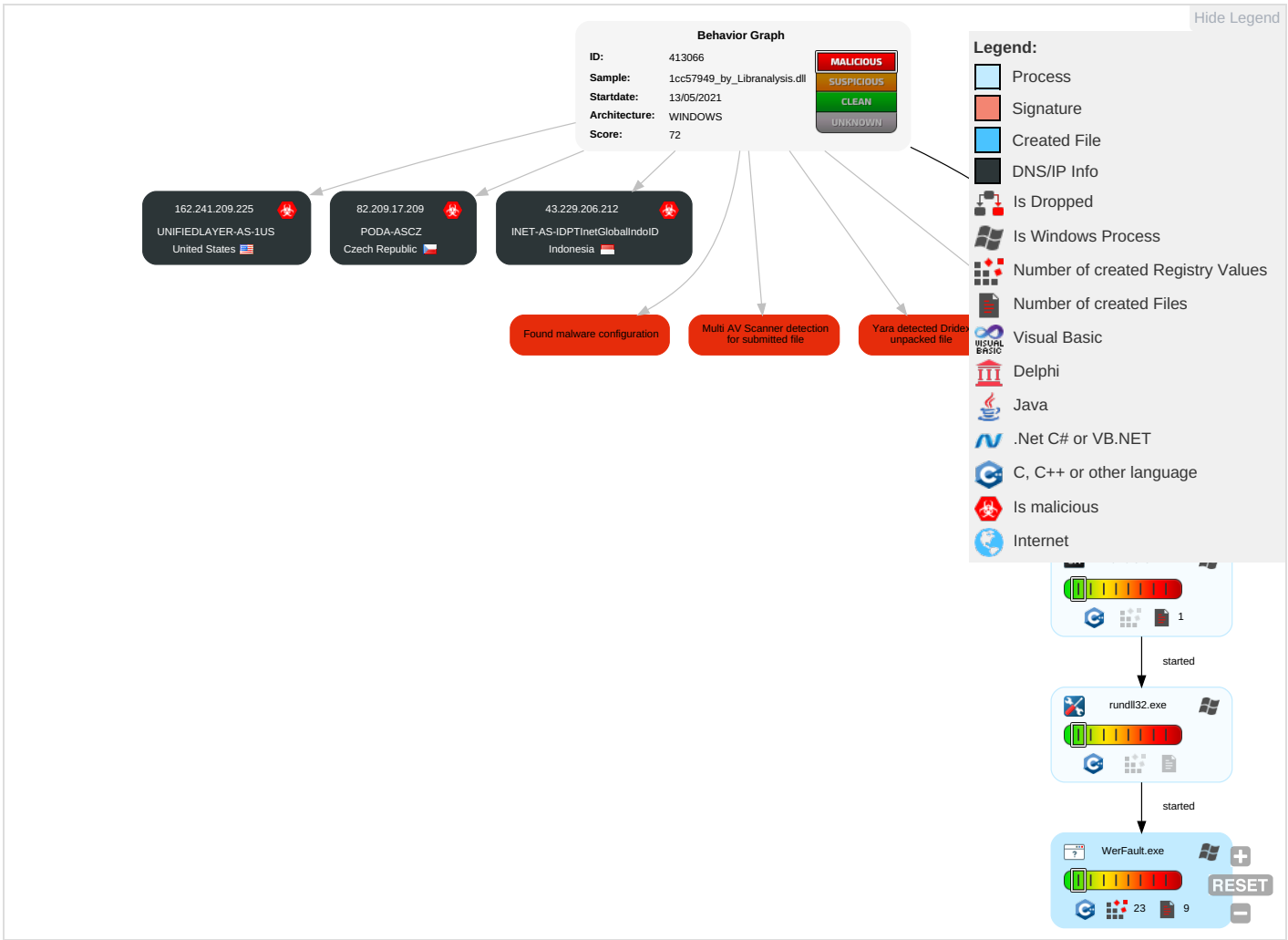
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati

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	Remote Desktop Protocol	Archive Collected Data 1	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

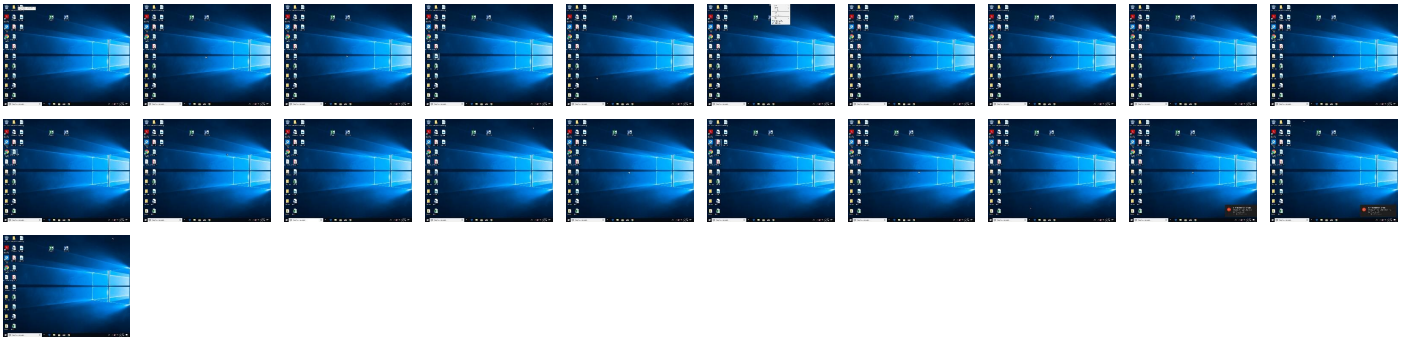
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1cc57949_by_Libranalysis.dll	38%	ReversingLabs	Win32.Trojan.Convagent	
1cc57949_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.980000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

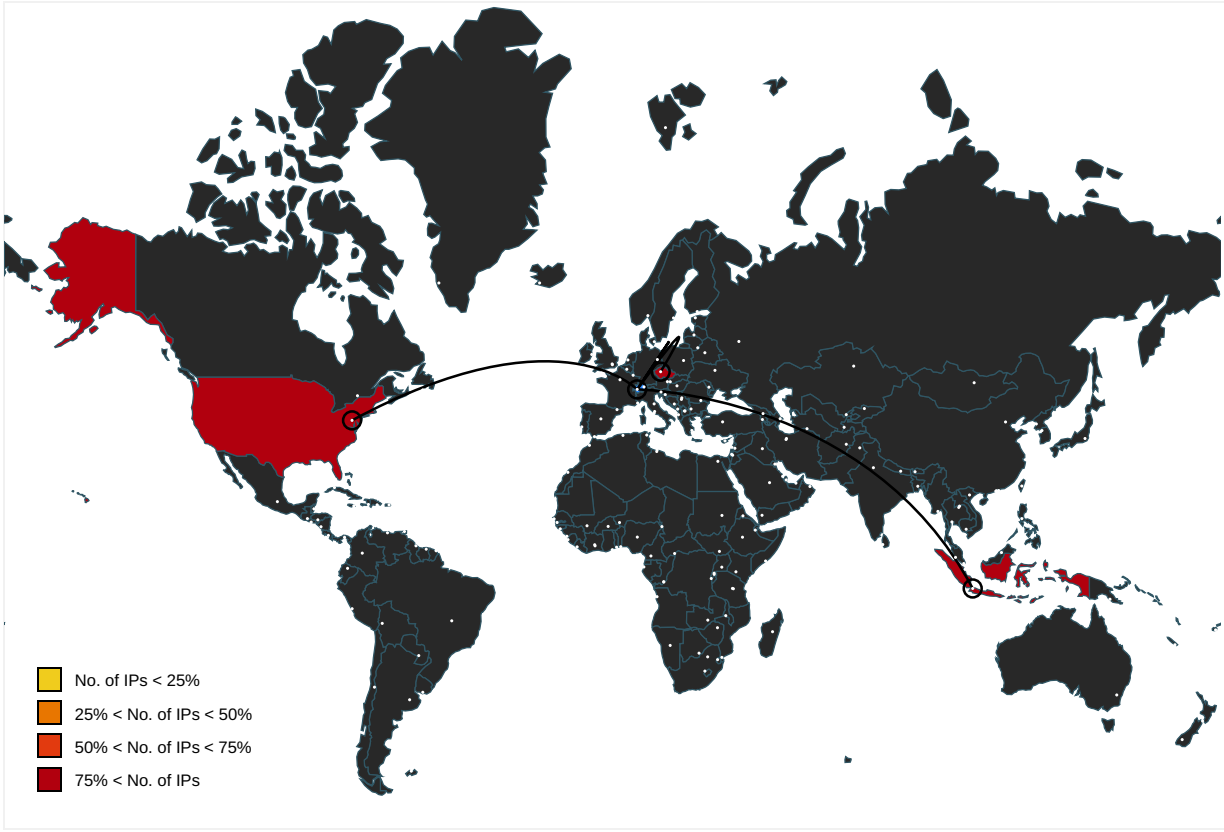
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413066
Start date:	13.05.2021

Start time:	07:32:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1cc57949_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@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.7% (good quality ratio 85.8%) • Quality average: 67.5% • Quality standard deviation: 34.8%
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	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_560fd288c3f3fcce8bd7ef2d777917589d96db_82810a17_107b61e5\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_560fd288c3f3fcce8bd7ef2d777917589d96db_82810a17_107b61e5\Report.wer	
Category:	dropped
Size (bytes):	12484
Entropy (8bit):	3.7685157989560882
Encrypted:	false
SSDEEP:	192:7UCiC0oXv3cHBUZMX4jed+Q3G/u7seS274ItWcf:wCiEXvUBUZMX4je1W/u7seX4ItWcf
MD5:	9F0B236E953EE300C5F6AA1CEC08C5C6
SHA1:	9713512E7052AE002A07FDA45DC82CBDD94CB31E
SHA-256:	FA57746CA6D2E5FC0A98F047F1D314E2D7A28AD0CDEAB5B1145140E3DB2AC04B
SHA-512:	860008AB858BEB0D0FDAADBE7BB94D9D96C6F64B4040E004B78E7F863B96EB844AA691A43FAB801F10F903364DE095E27D3B8344AE1059980F1A68C6E3464A6A
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.9.0.0.6.1.5.2.5.3.1.5.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.9.0.0.6.3.5.2.5.3.1.0.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.1.7.6.9.2.6.9.-.f.d.5.4.-.4.9.1.a.-.8.4.8.c.-.9.c.9.2.8.b.5.2.7.1.a.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.d.c.2.9.1.7.c.b.-.2.1.e.3.-.4.6.f.5.-.b.b.4.3.-.5.5.b.3.7.4.9.0.3.3.e.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.6.8.-.0.0.0.1.-.0.0.1.7.-.3.2.8.a.-.d.f.f.d.0.4.4.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:34:22 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46762
Entropy (8bit):	2.1110582536596567
Encrypted:	false
SSDEEP:	192:4gzvCb8+eMThaSvTM1Cb/3fCZzBDdH8Tt3tTrjKMKSnFsn:TCQM9aSvT4Cb3+jH8TttrjKUY
MD5:	04622FD2B37A3192FA92A163CD774BEF
SHA1:	A47B2B173B246D8B10CCEC520D4CBFF1708AA3D9
SHA-256:	A8D7200305AAEDDCFF92D40580B19DD37FF51FE0FEBE59BC4AB02A791BD51654
SHA-512:	5A58458516010E19CE22C073939D371B12E099C987C34D51D84C0A83384B644DE11A52B637C9709CFE445305A597C58ABF4851556FFB3D202A931A0905EF9FE9
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....8.`.....U.....B.....GenuineIntelW.....T.....h....8.`.....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\WER539D.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):	3.6929302971334503
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipcs6w6YfK62FgmfT0G3VSGCprc89buusf0706m:RrlsNipf6w6YC62FgmfT0GlSnutfw4
MD5:	5F4577F30AF8E84A59F35827811B5425
SHA1:	184C5607025349FBC8DAD871B5597F9E713ABE86
SHA-256:	90DA42AB471C85C308C9DEFF00E390B9A15BD7AF31F2F13513FAA32DA7690651
SHA-512:	2A302CCDC6A2EED90513D459C7710D93575096E0F177DA3D3EB775C4DD822650F548E4111E54CD442BF7091F3DF6258F01B67CA235332490F3712C47F7AE8A4E
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5535.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):	4.472285095471318

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5535.tmp.xml	
Encrypted:	false
SSDEEP:	48:cvIwSD8zsJJgtWI9z/7WSC8Bd/8fm8M4JCdsfNrFv+q8/GNF+4SrSOd:uITfb0KSN0J9N1tNYDWOd
MD5:	16C2CF51C52AA14E87C3A2C6A444EFCE
SHA1:	752360F05D651D479A76E921B14DC78335BE62B0
SHA-256:	1524F36EBB699D9756378BD2FAC530684A58235B561E814764344686941FC1C1
SHA-512:	00C3889F009E672DFAE5EBEC2E58B5A57AD8C12591EFF8CEC1B974D86C5818321800C8EECEF6227770DCBD45B122B45FEA0AA1AB35A78E447E696417D3A9118
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="987825" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.513859882427295
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:	1cc57949_by_Libranalysis.dll
File size:	167424
MD5:	1cc57949b45974cc40c409810528521b
SHA1:	0dceb93b98a9bc26759c73d78fe9a9d4f56b8e61
SHA256:	814739bdf67c1f2330a9f876e1c50af7b64c697462ddfecc02225bb8880168c7
SHA512:	e90ae803c69aa22df6ea68564fa1b09e5d7225dc85df529fe66ab89d5470bdbba514cc0bb3903e21d4a0453ce08e3e115b4b3c65730313d3ba23de5154ef7395
SSDEEP:	3072:49F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:49F6rQXvFczvYpQP
File Content Preview:	MZ.....@.....\.....!..L.!This 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:	0x609C8025 [Thu May 13 01:25:57 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0

General

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 00007F169501BDB6h
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
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

Name	Virtual Address	Virtual Size	Is in Section
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	0x23e44	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	0x34d0	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
.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

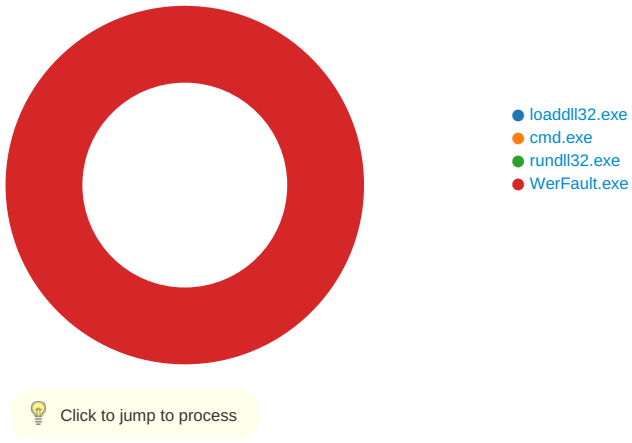
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:33:41.591975927 CEST	49199	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:41.641557932 CEST	53	49199	8.8.8.8	192.168.2.3
May 13, 2021 07:33:42.613066912 CEST	50620	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:42.664489031 CEST	53	50620	8.8.8.8	192.168.2.3
May 13, 2021 07:33:42.951466084 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:43.012475967 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 07:33:43.572364092 CEST	60152	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:43.633867025 CEST	53	60152	8.8.8.8	192.168.2.3
May 13, 2021 07:33:44.399521112 CEST	57544	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:44.452768087 CEST	53	57544	8.8.8.8	192.168.2.3
May 13, 2021 07:33:45.167108059 CEST	55984	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:45.227324963 CEST	53	55984	8.8.8.8	192.168.2.3
May 13, 2021 07:33:46.157191992 CEST	64185	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:46.214385033 CEST	53	64185	8.8.8.8	192.168.2.3
May 13, 2021 07:33:47.409368038 CEST	65110	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:47.457976103 CEST	53	65110	8.8.8.8	192.168.2.3
May 13, 2021 07:33:48.427591085 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:48.476758003 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 07:33:49.566800117 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:49.615525007 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 07:33:50.535202980 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:50.585758924 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 07:33:52.035649061 CEST	60100	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:52.094631910 CEST	53	60100	8.8.8.8	192.168.2.3
May 13, 2021 07:33:53.996325970 CEST	53195	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:54.048278093 CEST	53	53195	8.8.8.8	192.168.2.3
May 13, 2021 07:33:55.161276102 CEST	50141	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:55.210024118 CEST	53	50141	8.8.8.8	192.168.2.3
May 13, 2021 07:33:56.112329960 CEST	53023	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:56.161150932 CEST	53	53023	8.8.8.8	192.168.2.3
May 13, 2021 07:33:57.534955025 CEST	49563	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:57.585099936 CEST	53	49563	8.8.8.8	192.168.2.3
May 13, 2021 07:33:58.444654942 CEST	51352	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:58.493350983 CEST	53	51352	8.8.8.8	192.168.2.3
May 13, 2021 07:33:59.374737978 CEST	59349	53	192.168.2.3	8.8.8.8
May 13, 2021 07:33:59.423340082 CEST	53	59349	8.8.8.8	192.168.2.3
May 13, 2021 07:34:01.281861067 CEST	57084	53	192.168.2.3	8.8.8.8
May 13, 2021 07:34:01.330688000 CEST	53	57084	8.8.8.8	192.168.2.3
May 13, 2021 07:34:11.050395012 CEST	58823	53	192.168.2.3	8.8.8.8
May 13, 2021 07:34:11.127362013 CEST	53	58823	8.8.8.8	192.168.2.3
May 13, 2021 07:34:24.144217014 CEST	57568	53	192.168.2.3	8.8.8.8
May 13, 2021 07:34:24.201504946 CEST	53	57568	8.8.8.8	192.168.2.3
May 13, 2021 07:34:25.974754095 CEST	50540	53	192.168.2.3	8.8.8.8
May 13, 2021 07:34:26.031719923 CEST	53	50540	8.8.8.8	192.168.2.3
May 13, 2021 07:34:31.918169975 CEST	54366	53	192.168.2.3	8.8.8.8
May 13, 2021 07:34:31.976610899 CEST	53	54366	8.8.8.8	192.168.2.3
May 13, 2021 07:34:37.388178110 CEST	53034	53	192.168.2.3	8.8.8.8
May 13, 2021 07:34:37.447402954 CEST	53	53034	8.8.8.8	192.168.2.3
May 13, 2021 07:35:04.172322035 CEST	57762	53	192.168.2.3	8.8.8.8
May 13, 2021 07:35:04.229867935 CEST	53	57762	8.8.8.8	192.168.2.3
May 13, 2021 07:35:09.508359909 CEST	55435	53	192.168.2.3	8.8.8.8
May 13, 2021 07:35:09.565845966 CEST	53	55435	8.8.8.8	192.168.2.3
May 13, 2021 07:35:25.128880978 CEST	50713	53	192.168.2.3	8.8.8.8
May 13, 2021 07:35:25.201800108 CEST	53	50713	8.8.8.8	192.168.2.3
May 13, 2021 07:35:39.986742973 CEST	56132	53	192.168.2.3	8.8.8.8
May 13, 2021 07:35:40.044154882 CEST	53	56132	8.8.8.8	192.168.2.3
May 13, 2021 07:35:41.823417902 CEST	58987	53	192.168.2.3	8.8.8.8
May 13, 2021 07:35:41.883341074 CEST	53	58987	8.8.8.8	192.168.2.3
May 13, 2021 07:36:27.939547062 CEST	56579	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:36:27.998826027 CEST	53	56579	8.8.8.8	192.168.2.3
May 13, 2021 07:36:28.677074909 CEST	60633	53	192.168.2.3	8.8.8.8
May 13, 2021 07:36:28.736326933 CEST	53	60633	8.8.8.8	192.168.2.3
May 13, 2021 07:36:29.433021069 CEST	61292	53	192.168.2.3	8.8.8.8
May 13, 2021 07:36:29.490447044 CEST	53	61292	8.8.8.8	192.168.2.3
May 13, 2021 07:36:30.194576979 CEST	63619	53	192.168.2.3	8.8.8.8
May 13, 2021 07:36:30.254132986 CEST	53	63619	8.8.8.8	192.168.2.3
May 13, 2021 07:36:31.012599945 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 07:36:31.072551966 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 07:36:31.698257923 CEST	61946	53	192.168.2.3	8.8.8.8
May 13, 2021 07:36:31.756052017 CEST	53	61946	8.8.8.8	192.168.2.3
May 13, 2021 07:36:32.257061005 CEST	64910	53	192.168.2.3	8.8.8.8
May 13, 2021 07:36:32.314148903 CEST	53	64910	8.8.8.8	192.168.2.3
May 13, 2021 07:36:33.213530064 CEST	52123	53	192.168.2.3	8.8.8.8
May 13, 2021 07:36:33.262547970 CEST	53	52123	8.8.8.8	192.168.2.3
May 13, 2021 07:36:34.265305996 CEST	56130	53	192.168.2.3	8.8.8.8
May 13, 2021 07:36:34.314141989 CEST	53	56130	8.8.8.8	192.168.2.3
May 13, 2021 07:36:34.963531017 CEST	56338	53	192.168.2.3	8.8.8.8
May 13, 2021 07:36:35.020801067 CEST	53	56338	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 2168 Parent PID: 5616

General

Start time:	07:33:50
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\1cc57949_by_Libranalysis.dll'

Imagebase:	0x370000
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: 6064 Parent PID: 2168

General

Start time:	07:33:50
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\1cc57949_by_Libranalysis.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5992 Parent PID: 6064

General

Start time:	07:33:50
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\1cc57949_by_Libranalysis.dll',#1
Imagebase:	0x10e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.301331659.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 4120 Parent PID: 5992

General

Start time:	07:34:20
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5992 -s 764
Imagebase:	0xb00000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	701D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5535.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5535.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_560fd288c3f3fcce8bd7ef2d777917589d96db_82810a17_107b61e5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_560fd288c3f3fcce8bd7ef2d777917589d96db_82810a17_107b61e5\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	701C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5535.tmp	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	success or wait	1	701C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	success or wait	1	701C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5535.tmp.xml	success or wait	1	701C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER167E.tmp.csv	success or wait	1	701C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER173A.tmp.txt	success or wait	1	701C4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 ee 38 9d 60 a4 05 12 00 00 00 00 00	MDMP........ ....8.`........	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	6	00 00 00 00 00 00	......	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 a8 1f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 68 17 00 00 ce 38 9d 60 07 00 00 00 11 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....h....8.`.................. ....0..=............... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e................... ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 ca 30 00 10 20 35 9a 00 ff ff ff ff ca 30 00 10 19 06 00 02 14 f8 50 00 ca 30 00 10 23 00 00 00 03 02 01 00 90 f7 50 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........0.. 5.......0...... ..P..0..#.........P.+.........	success or wait	1	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	168	c8 06 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 7c 25 00 00	........................0.... ....|%..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	20	0e 00 00 00 94 fb ac 00 00 00 00 00 6c 04 00 00 90 31 00 00	...........l....1..	success or wait	14	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	1132	bc b1 e5 77 d6 c9 e3 77 64 02 00 00 aa aa aa aa 10 00 00 00 28 fc ac 00 f4 fc ac 00 aa aa aa aa 40 c7 e3 77 40 c7 e3 77 aa aa aa aa 00 40 6f 00 00 40 6f 00 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 40 6f 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa b8 68 9a 00 00 00 00 00 00 00 00 00 b0 08 9a 00 00 b0 6e 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 54 b2 6e 00 4c fa 91 00 48 07 9a 00 54 fa 91 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...wd...........(......... ..@..w@..w.....@o..@o..... d.......d........@o.............. ....h.... ....n................. ....T.n.L. ..H...T......................	success or wait	13	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	4096	40 fd ac 00 00 00 ad 00 00 40 ac 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 40 6f 00 00 00 00 00 68 17 00 00 c8 0b 00 00 00 00 00 00 00 00 00 00 00 b0 6e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 d6 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@........@...............@o... ..h.................n......... ....p.w..............	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 aa aa aa aa ca 30 00 10 00 00 00 00 28 e9 50 00 bc 9a e5 77 23 00 00 00 02 02 00 00 98 e7 50 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................. ....+...S...+. ..+....................0...... (.P....w#.........P.+.........	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	48	c8 0b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 40 6f 00 00 00 00 00 94 fb ac 00 00 00 00 00 6c 04 00 00 90 31 00 00 cc 02 00 00 e0 2d 00 00	....@o........... ..l....1.......-..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	....r.u.n.d.l.l.3.2...e.x.e...	success or wait	51	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 62 25 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 60 22 02 00 00 00 00 00 a0 bb 02 00 00 00 00 6c 55 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 a8 ee 00 00 00 00 00 00 5f 63 03 00 00 00 00 00 23 91 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 d8 d6 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 d9 de 21 00 00 00 00	..Ht.....0...U..s@..b%.....B.....B?.....#.....@A.....Zb.....`".....IU....._c.....#.....!.....@.....!....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t.....F.i.l.e.....F.i.l.e...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m	success or wait	1	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4FB4.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 9c 07 00 00 05 00 00 00 e4 00 00 00 ac 30 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 92 98 00 00 15 00 00 00 ec 01 00 00 24 1d 00 00 16 00 00 00 98 00 00 00 10 1f 00 00	....0.....T.....8..... ....T.....`..... ..$.....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.9.9.2.<./.P.i.d.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.l.l.3.2...e.x.e.<./.I.m.a.g.e.N.a.m.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 31 00 38 00 36 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.1.8.6.4.<./.U.p.t.i.m.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 32 00 39 00 39 00 35 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.2.9.9.5.8.4.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 32 00 39 00 31 00 33 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.2.9.1.3.9.2.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 38 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.6.8.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 30 00 33 00 37 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.0.3.7.1.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 30 00 33 00 37 00 31 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.>.9.2.0.3.7.1.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.4.1.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 30 00 38 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.>.3.0.0.8.8.<./.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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 38 00 31 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.>.2.9.8.1.6.<./.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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 38 00 37 00 36 00 34 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.7.8.7.6.4.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 37 00 39 00 35 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.7.9.5.8.4.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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 38 00 37 00 36 00 34 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.7.8.7.6.4.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.0.6.4.<./.P.i.d.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0. <./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 32 00 32 00 31 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.2.2.1.4. <./.U.p.t.i.m.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<.I.p.t.E.n.a.b.l.e.d.>.0.<./.I.p.t.E.n.a.b.l.e.d.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 31 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.1.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 31 00 35 00 30 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.1.5.0.7.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 37 00 38 00 32 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.7.8.2.0.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.9.5.2.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 31 00 30 00 31 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.1.0.1.4.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 36 00 33 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.6.3.5.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 31 00 30 00 31 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.1.0.1.4.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./.P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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 61 00 6d 00 72 00 73 00 74 00 65 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.a.m.r.s.t.e.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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 61 00 6d 00 72 00 73 00 74 00 65 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.>.a.m.r.s.t.e.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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 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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 38 00 35 00 30 00 33 00 33 00 30 00 39 00 37 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.8.5.0.3.3.0.9.7.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 33 00 34 00 3a 00 32 00 32 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.1.4.:.3.4.:.2.2.Z.".>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 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 32 00 38 00 36 00 35 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 38 00 36 00 35 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.4.6.". .P.I.D.=.".5.9.9.2.". .U.p.t.i.m.e.M.S.=.".2.8.6.5.6.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.8.6.5.6.". .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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 31 00 37 00 36 00 39 00 32 00 36 00 39 00 2d 00 66 00 64 00 35 00 34 00 2d 00 34 00 39 00 31 00 61 00 2d 00 38 00 34 00 38 00 63 00 2d 00 39 00 63 00 39 00 32 00 38 00 62 00 35 00 32 00 37 00 31 00 61 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.a.1.7.6.9.2.6.9.-.f.d.5.4.-.4.9.1.a.-.8.4.8.c.-.9.c.9.2.8.b.5.2.7.1.a.e.<./.G.u.i.d.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 33 00 34 00 3a 00 32 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.4.:.3.4.:.2.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER539D.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	701C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5535.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	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_560fd288c3f3fcce8bd7ef2d777917589d96db_82810a17_107b61e5\Report.wer	unknown	2	ff fe	..	success or wait	1	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_560fd288c3f3fcce8bd7ef2d777917589d96db_82810a17_107b61e5\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	182	701C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_560fd288c3f3fcce8bd7ef2d777917589d96db_82810a17_107b61e5\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 34 00 30 00 38 00 38 00 30 00 36 00 33 00 35 00 30 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.4.0.8.8.0.6.3.5.0.	success or wait	1	701C497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	701E36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	701E1FB2	RegCreateKeyExW
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	701C43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	701E36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	701E36BF	unknown
\REGISTRY\A\{06854bb5-b7bb-13ab-d30f-f73af21a23e4}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	701E36BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 CA 30 00 10 02 00 00 00 01 00 00 00 19 06 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	701E1FE8	RegSetValueExW

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

Disassembly

Code Analysis