ID: 413059
Sample Name:
2a71d07d_by_Libranalysis
Cookbook: default.jbs
Time: 07:14:42
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

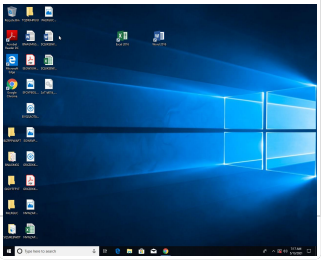
Analysis Report 2a71d07d_by_Libranalysis

Overview

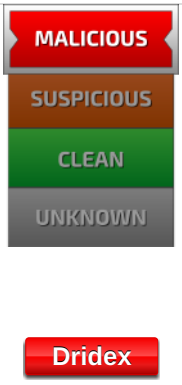
General Information

Sample Name:	2a71d07d_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	413059
MD5:	2a71d07d2558a0..
SHA1:	0515ca7e2258c3..
SHA256:	0e3d0e409a4a46..
Infos:	

Most interesting Screenshot:



Detection

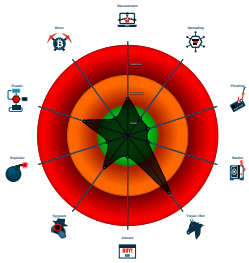


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Dridex unpacked file
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Checks if the current process is bein…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function
- IP address seen in connection with o…
- Internet Provider seen in connection…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 4168 cmdline: loaddll32.exe 'C:\Users\user\Desktop\2a71d07d_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4856 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2a71d07d_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3636 cmdline: rundll32.exe 'C:\Users\user\Desktop\2a71d07d_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 4608 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 3636 -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
00000002.00000002.293111007.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

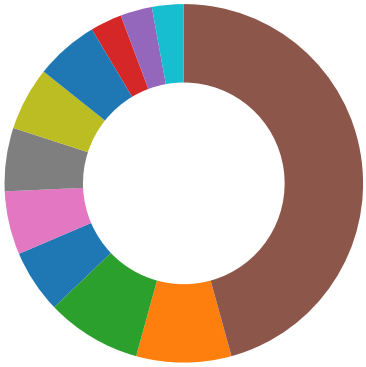
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- 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

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

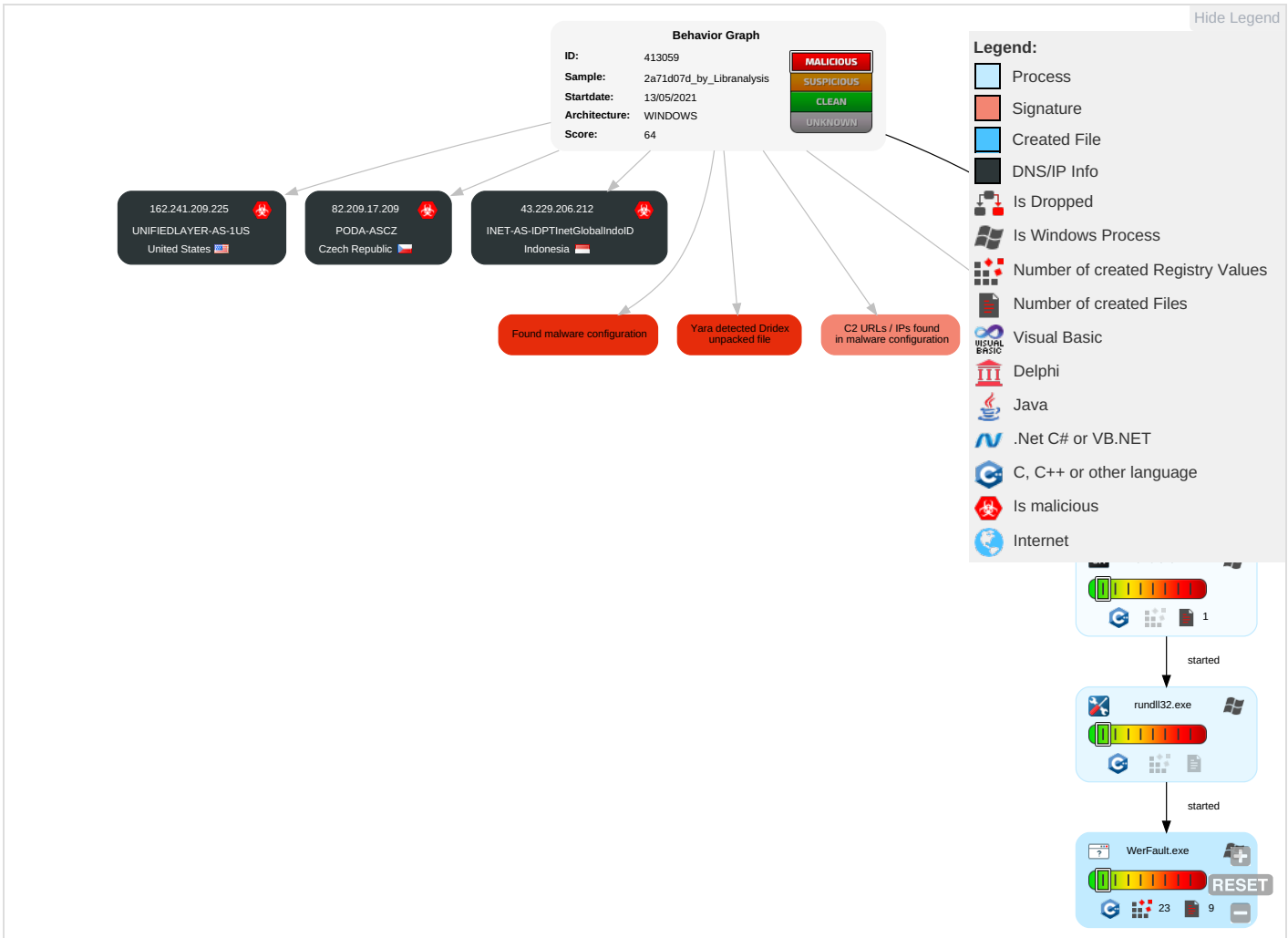
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 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

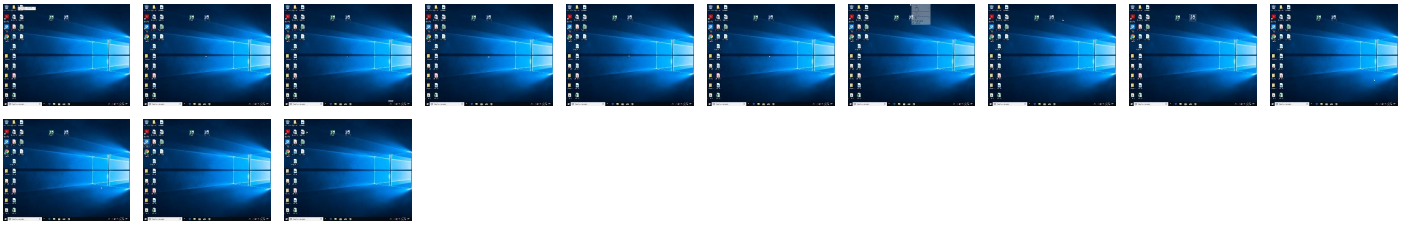
Behavior Graph



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
2a71d07d_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.d80000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

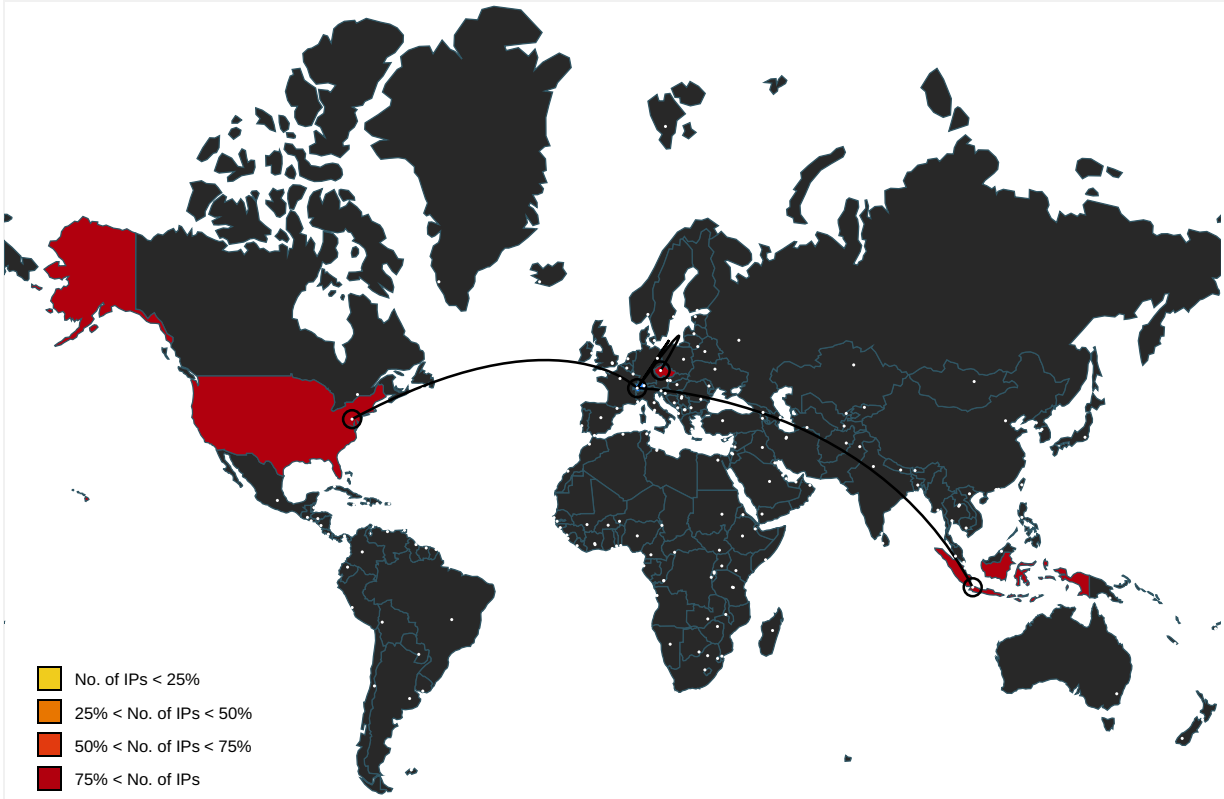
No Antivirus matches

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:	413059
Start date:	13.05.2021
Start time:	07:14:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	2a71d07d_by_Libranalysis (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 57% (good quality ratio 49.4%) • Quality average: 67.4% • Quality standard deviation: 35.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Simulations

Behavior and APIs

Time	Type	Description
07:16:12	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.209.225	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5e32d1e1b3525e7c67f78118fab6586a885e36df_82810a17_126713a2\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12482
Entropy (8bit):	3.767518431933883
Encrypted:	false
SSDEEP:	192:4WU9ie0oXUwcHBUZMX4jed+1G/u7suS274ItWch:AioXUrBUZMX4je5/u7suX4ItWch
MD5:	1128034D840B45B6ECA7DE2B7EC8F785
SHA1:	D0B0B9868B885E97D464610B96F5F58C2659F2F1
SHA-256:	319E26273BABA0EF4FC999ED343995B391564D1A0310931FC92774A5E42E613A

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5e32d1e1b3525e7c67f78118fab6586a885e36df_82810a17_126713a2\Report.wer	
SHA-512:	7785AE36B27E5A637FB3190B2E4500E486C7B1F50496AB37C0C75CC14C84B3C04F1668DB3698D20E01862814172E8DC34F7D6A134BD4855C17247194FA755D9E
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.8.8.9.6.9.2.2.9.5.8.3.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.8.8.9.7.1.3.7.0.2.0.1.5.....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.=.c.3.7.6.a.6.c.f.-.d.8.f.5.-.4.a.6.b.-.a.c.7.a.-.2.b.5.2.4.5.0.5.e.4.e.4.....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.5.0.c.c.3.8.8.-.3.3.6.6.-.4.8.7.e.-.a.1.8.1.-.7.2.3.b.c.6.8.f.4.a.5.8.....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.=.0.0.0.0.0.e.3.4.-.0.0.0.1.-.0.0.1.7.-.0.5.a.8.-.3.a.7.1.0.2.4.8.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\WER8FCC.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:16:10 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46118
Entropy (8bit):	2.1468042056124736
Encrypted:	false
SSDEEP:	192:0RzYUkaAbrgGvOvcQCK4HkfCZeBDdHY+HhxuGNid193nHSR:NUkasrGUQGHW+gHY+vuGNInA
MD5:	38AA790B7AC1D1FE03058091CAB7B07B
SHA1:	E827408FCD07DBD11674AFB37AD1675CED0E650A
SHA-256:	85881E3AD823D9F8B2AAD24E16FED5403EF0C45053FAEA39286552E62656B418
SHA-512:	F3F1A4EF60BCAFAE154CA79427F0E2B7E00287CF1ACC077A57C12F62A3ADC55F35205C598A20E5C3F7622F4D58DE3FDDBF09C9959B795D50350D57C337A5123
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....4.`.....U.....B.....GenuineIntelW.....T.....4....4.`.....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\WER9413.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):	3.693617165616258
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNitw6Z6Yse64igmfTQVSbCpr189bfn5sfx1m:RrlsNiq6Z6Y964igmfTQShfnSfa
MD5:	CF51C1B0A367440743AC0A9B6A1A4F65
SHA1:	868B74E9D15997E03267A5FA46192B73EFBAD4A4
SHA-256:	C33CCB28F60507A186C5BBC0C6DFBD86A6D264F0CA58CAAEA7E41FB5B3D1BE70
SHA-512:	CA3D48C14F3205CF879377DC6E65740680B24243B925B03FD351EF6F9E479E095F9D117DEDBE08CD3994606971BE4F1D32333457B262C15EF13F156B70E2B6A3
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.>.3.6.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER953D.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):	4.471533686853024
Encrypted:	false
SSDEEP:	48:cvIwSD8zsOJgtWI9hFWSC8BS8fm8M4JCdsiNrF1D+q8/PNF+4SrSYd:uITfE+0SN1JoNHD4NoDWYd
MD5:	18E8B898F05B5C3DD9AFCF487DA10200
SHA1:	4306199D33720C31A4EA77DCB6222A95F668EA85
SHA-256:	941202C23FAFC31BE9C838DF6A64F37EA50A584EECF22FE2C0110397A87852F5
SHA-512:	02CE8355E7EFB46CAE97DA64421CD43B06C12CC714161432F299A1DC80D0197CAE75E20ACEF9EC042B9FB4640F4E9AF9266C5972232C3FDE65568084C06C0EB
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER953D.tmp.xml	
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="987806" />.. <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):	7.513869948958515
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:	2a71d07d_by_Libranalysis.dll
File size:	167424
MD5:	2a71d07d2558a0bb9ab701c68b2b7009
SHA1:	0515ca7e2258c364699bbaa6cd1ac7931cd092a1
SHA256:	0e3d0e409a4a46dec0ba0c9e15aff19f75b3b70d41997a9e56f89e97ee64e614
SHA512:	efc3088868a6e785dd1f7a0e6d71e734635fef56c2922a82e478fbacc0eaf2690261cad1f89272847f83b7678a4458c68ee90bb811df359e69e97e6fa755e7ac
SSDEEP:	3072:x9F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:x9F6rQXvFczvYpQP
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:	0x609C8023 [Thu May 13 01:25:55 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	88962f6760ea005847fb88b87e8ce1fd

Entrypoint Preview

Instruction
mov eax, 00000000h
cmpss xmm1, xmm2, 03h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp eax, 02h
mov eax, ebp
mov dword ptr [10029734h], eax
mov eax, ebx
mov dword ptr [10029730h], eax
mov eax, esi
mov dword ptr [10029728h], eax
jne 00007FEDE101A706h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Rich Headers

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

Data Directories

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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x4c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x23dfe	0x23e00	False	0.756362968206	data	7.53078515147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x389c	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x3a0	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.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

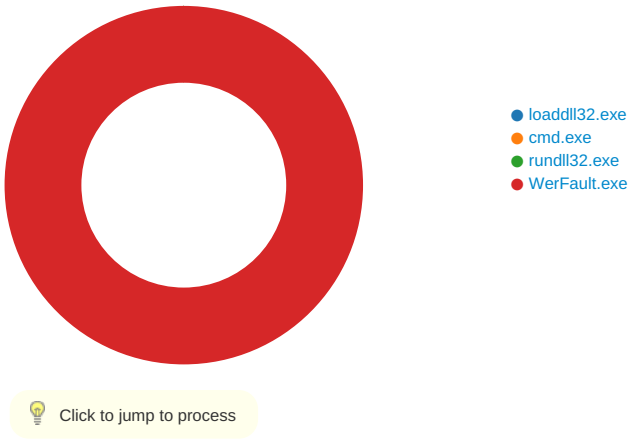
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:15:26.686638117 CEST	53	51281	8.8.8.8	192.168.2.3
May 13, 2021 07:15:26.688520908 CEST	49199	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:26.702251911 CEST	50620	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:15:26.737206936 CEST	53	49199	8.8.8.8	192.168.2.3
May 13, 2021 07:15:26.777293921 CEST	53	50620	8.8.8.8	192.168.2.3
May 13, 2021 07:15:26.909348965 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:26.969623089 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 07:15:27.443077087 CEST	60152	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:27.495605946 CEST	53	60152	8.8.8.8	192.168.2.3
May 13, 2021 07:15:29.982964993 CEST	57544	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:30.044810057 CEST	53	57544	8.8.8.8	192.168.2.3
May 13, 2021 07:15:30.849426031 CEST	55984	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:30.902123928 CEST	53	55984	8.8.8.8	192.168.2.3
May 13, 2021 07:15:31.857415915 CEST	64185	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:31.906342030 CEST	53	64185	8.8.8.8	192.168.2.3
May 13, 2021 07:15:32.874978065 CEST	65110	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:32.932156086 CEST	53	65110	8.8.8.8	192.168.2.3
May 13, 2021 07:15:39.983567953 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:40.032356977 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 07:15:40.786495924 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:40.835283995 CEST	53	63492	8.8.8.8	192.168.2.3
May 13, 2021 07:15:41.896287918 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:41.946419001 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 07:15:42.841459990 CEST	60100	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:42.898762941 CEST	53	60100	8.8.8.8	192.168.2.3
May 13, 2021 07:15:43.830533028 CEST	53195	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:43.890641928 CEST	53	53195	8.8.8.8	192.168.2.3
May 13, 2021 07:15:45.443512917 CEST	50141	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:45.492244005 CEST	53	50141	8.8.8.8	192.168.2.3
May 13, 2021 07:15:46.567153931 CEST	53023	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:46.615864038 CEST	53	53023	8.8.8.8	192.168.2.3
May 13, 2021 07:15:47.362550974 CEST	49563	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:47.411397934 CEST	53	49563	8.8.8.8	192.168.2.3
May 13, 2021 07:15:48.616920948 CEST	51352	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:48.675738096 CEST	53	51352	8.8.8.8	192.168.2.3
May 13, 2021 07:15:54.693469048 CEST	59349	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:54.742096901 CEST	53	59349	8.8.8.8	192.168.2.3
May 13, 2021 07:15:55.504951000 CEST	57084	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:55.553744078 CEST	53	57084	8.8.8.8	192.168.2.3
May 13, 2021 07:15:56.299130917 CEST	58823	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:56.349631071 CEST	53	58823	8.8.8.8	192.168.2.3
May 13, 2021 07:15:58.119261026 CEST	57568	53	192.168.2.3	8.8.8.8
May 13, 2021 07:15:58.176493883 CEST	53	57568	8.8.8.8	192.168.2.3
May 13, 2021 07:16:00.198702097 CEST	50540	53	192.168.2.3	8.8.8.8
May 13, 2021 07:16:00.257688046 CEST	53	50540	8.8.8.8	192.168.2.3
May 13, 2021 07:16:10.271420002 CEST	54366	53	192.168.2.3	8.8.8.8
May 13, 2021 07:16:10.338891983 CEST	53	54366	8.8.8.8	192.168.2.3
May 13, 2021 07:16:11.612138033 CEST	53034	53	192.168.2.3	8.8.8.8
May 13, 2021 07:16:11.662036896 CEST	53	53034	8.8.8.8	192.168.2.3
May 13, 2021 07:16:19.080435038 CEST	57762	53	192.168.2.3	8.8.8.8
May 13, 2021 07:16:19.141362906 CEST	53	57762	8.8.8.8	192.168.2.3
May 13, 2021 07:16:22.187797070 CEST	55435	53	192.168.2.3	8.8.8.8
May 13, 2021 07:16:22.236650944 CEST	53	55435	8.8.8.8	192.168.2.3
May 13, 2021 07:16:49.881880045 CEST	50713	53	192.168.2.3	8.8.8.8
May 13, 2021 07:16:49.946985960 CEST	53	50713	8.8.8.8	192.168.2.3
May 13, 2021 07:16:55.901968956 CEST	56132	53	192.168.2.3	8.8.8.8
May 13, 2021 07:16:55.961009026 CEST	53	56132	8.8.8.8	192.168.2.3
May 13, 2021 07:17:16.144573927 CEST	58987	53	192.168.2.3	8.8.8.8
May 13, 2021 07:17:16.214315891 CEST	53	58987	8.8.8.8	192.168.2.3
May 13, 2021 07:17:24.808646917 CEST	56579	53	192.168.2.3	8.8.8.8
May 13, 2021 07:17:24.875758886 CEST	53	56579	8.8.8.8	192.168.2.3
May 13, 2021 07:17:27.004266024 CEST	60633	53	192.168.2.3	8.8.8.8
May 13, 2021 07:17:27.069664955 CEST	53	60633	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 4168 Parent PID: 5600

General

Start time:	07:15:35
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\2a71d07d_by_Libranalysis.dll'
Imagebase:	0xa60000
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: 4856 Parent PID: 4168

General

Start time:	07:15:35
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\2a71d07d_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: 3636 Parent PID: 4856

General

Start time:	07:15:35
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\2a71d07d_by_Libranalysis.dll',#1
Imagebase:	0xe90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.293111007.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 4608 Parent PID: 3636

General

Start time:	07:16:07
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 3636 -s 764
Imagebase:	0xcc0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70851717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER953D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER953D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5e32d1e1b3525e7c67f78118fab6586a885e36df_82810a17_126713a2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5e32d1e1b3525e7c67f78118fab6586a885e36df_82810a17_126713a2\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7084497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER953D.tmp	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	success or wait	1	70844BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	success or wait	1	70844BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER953D.tmp.xml	success or wait	1	70844BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER95E.tmp.csv	success or wait	1	70844BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER96F.tmp.txt	success or wait	1	70844BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 aa 34 9d 60 a4 05 12 00 00 00 00 00	MDMP..... .....4.`.....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.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 34 0e 00 00 87 34 9d 60 08 00 00 00 12 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 00 0b 00 00 00 01 00 02 00 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 00	.....U...........B............ ..GenuineIntelW...........T... ....4....4.`.................. ....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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.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 0b 03 ff ff ff ff ca 30 00 10 19 06 00 02 9c fc 9c 00 ca 30 00 10 23 00 00 00 03 02 01 00 18 fc 9c 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...... .....0..#...........+.........	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	168	84 10 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 cc 02 00 00 7c 25 00 00	.........................0.... ....|%..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	20	10 00 00 00 78 07 0a 03 00 00 00 00 04 00 00 00 b0 31 00 00	....x............1..	success or wait	16	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	4	f4 11 df 77	...w	success or wait	15	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	256	c2 10 00 90 b8 c4 01 00 00 ba e0 dc e6 77 ff d2 c2 0c 00 90 b8 c5 01 00 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 c6 01 00 00 ba e0 dc e6 77 ff d2 c2 1c 00 90 b8 c7 01 00 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 c8 01 06 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 c9 01 00 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 ca 01 15 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 cb 01 00 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 cc 01 03 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 cd 01 03 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 ce 01 00 00 ba e0 dc e6 77 ff d2 c2 14 00 90 b8 cf 01 00 00 ba e0 dc e6 77 ff d2 c3 8d 49 00 b8 d0 01 00 00 ba e0 dc e6 77 ff d2 c2 10 00 90 b8 d1 01 00 00 ba e0 dc e6 77 ff d2 c2 08 00 90 b8 d2 01 00 00 ba e0 dc e6 77 ff d2 c2 04 00 90 b8 d3 01 00 00 ba e0 dc e6 77 ff	............w...............w ....w............. .w..............w........... ...w..............w......... .....w..............w....... ....w..............w...... ....w....l..........w.... ....w..............w.. ....w.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	4	03 00 00 00	....	success or wait	3	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.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 b0 ed 9c 00 bc 9a e5 77 23 00 00 00 12 02 00 00 20 ec 9c 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 aa	?............................ ....+...S...+. ..+...................0...... ....w#....... ...+.........	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	48	18 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 b4 00 00 00 00 00 38 fa 8a 04 00 00 00 00 c8 05 00 00 44 81 00 00 cc 02 00 00 e0 2d 00 00	....P......8..... ......D........-..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.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	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.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 04 00 04 00 02 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 40 41 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 40 2c 02 00 00 00 00 00 b0 a8 02 00 00 00 00 d6 53 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 fc e6 00 00 00 00 00 00 f1 62 03 00 00 00 00 00 e3 90 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 2d d2 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 98 d7 21 00 00 00 00	..Ht.....0...U..s@..b%..... .....B.....B?..... .....#..... ..@A.....Zb..... ....@,..... .S.....b .....-.!..... @.....!....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t..... .....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(...W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t. .....I.R.T.i.m	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8FCC.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 04 01 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 0e 96 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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.6.3.6.<./.P.i.d.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 34 00 35 00 37 00 31 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.>.3.4.5.7.1.<./.U.p.t.i.m.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 30 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.6.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 39 00 35 00 35 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.9.5.5.2.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 39 00 35 00 35 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.9.5.5.2.0.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 31 00 32 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 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.>.3.0.1.2.0.<./.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 34 00 38 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.>.2.9.8.4.8.<./.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 38 00 30 00 38 00 31 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 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.>.5.8.0.8.1.2.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 38 00 31 00 36 00 33 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.>.5.8.1.6.3.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 38 00 30 00 38 00 31 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.8.0.8.1.2.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 38 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.8.5.6.<./.P.i.d.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 34 00 39 00 32 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.4.9.2.6.<./.U.p.t.i.m.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.2.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 32 00 37 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.2.7.3.6.0.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 39 00 30 00 34 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.9.0.4.9.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 30 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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 34 00 32 00 39 00 31 00 32 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.>.2.3.4.2.9.1.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 39 00 36 00 32 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.9.6.2.8.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 34 00 32 00 39 00 31 00 32 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.>.2.3.4.2.9.1.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 79 00 74 00 6b 00 72 00 73 00 79 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.>.y.t.k.r.s.y.,. .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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 79 00 74 00 6b 00 72 00 73 00 79 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.>.y.t.k.r.s.y.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n.>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./.B.I.O.S.V.e.r.s.i.o.n.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 35 00 36 00 35 00 32 00 32 00 38 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.6.5.6.5.2.2.8.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 31 00 36 00 3a 00 31 00 30 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.1.4.:.1.6.:.1.0.Z.".>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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 33 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 36 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 30 00 35 00 33 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 30 00 35 00 33 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 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.=.".3.3.9.". .P.I.D.=.".3.6.3.6.". .U.p.t.i.m.e.M.S.=.".3.0.5.3.1.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.0.5.3.1.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 33 00 37 00 36 00 61 00 36 00 63 00 66 00 2d 00 64 00 38 00 66 00 35 00 2d 00 34 00 61 00 36 00 62 00 2d 00 61 00 63 00 37 00 61 00 2d 00 32 00 62 00 35 00 32 00 34 00 35 00 30 00 35 00 65 00 34 00 65 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.c.3.7.6.a.6.c.f.-.d.8.f.5.-.4.a.6.b.-.a.c.7.a.-.2.b.5.2.4.5.0.5.e.4.e.4.<./.G.u.i.d.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 31 00 36 00 3a 00 31 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.4.:.1.6.:.1.0.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9413.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	7084497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER953D.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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5e32d1e1b3525e7c67f78118fab6586a885e36df_82810a17_126713a2\Report.wer	unknown	2	ff fe	..	success or wait	1	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5e32d1e1b3525e7c67f78118fab6586a885e36df_82810a17_126713a2\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	7084497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_5e32d1e1b3525e7c67f78118fab6586a885e36df_82810a17_126713a2\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 36 00 37 00 39 00 33 00 32 00 39 00 32 00 37 00 32 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.6.7.9.3.2.9.2.7.2.	success or wait	1	7084497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	708636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	70861FB2	RegCreateKeyExW
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	708443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	708636BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	708636BF	unknown
\REGISTRY\A\{5defe8ee-186f-4d2d-bddd-a03ff94a633d}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	708636BF	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	70861FE8	RegSetValueExW

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

Disassembly

Code Analysis