ID: 413054
Sample Name:
a194019c_by_Libranalysis
Cookbook: default.jbs
Time: 07:09:16
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

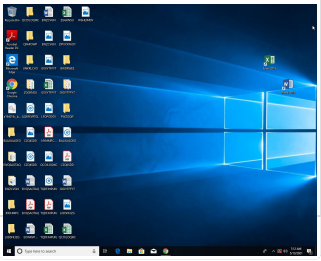
Analysis Report a194019c_by_Libranalysis

Overview

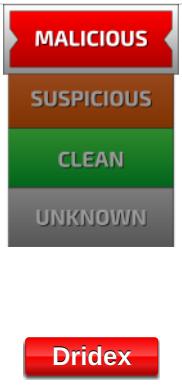
General Information

Sample Name:	a194019c_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	413054
MD5:	a194019cde6d13..
SHA1:	e6927771932bc0..
SHA256:	c7b86dcd1d64b9..
Infos:	

Most interesting Screenshot:



Detection

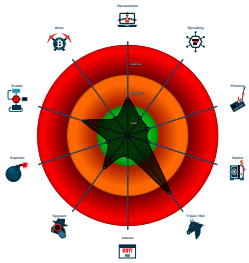


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 800 cmdline: loaddll32.exe 'C:\Users\user\Desktop\a194019c_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5700 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\a194019c_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5368 cmdline: rundll32.exe 'C:\Users\user\Desktop\a194019c_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6288 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5368 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22201,
  "C2 list": [
    "43.229.206.212:443",
    "82.209.17.209:8172",
    "162.241.209.225:4125"
  ],
  "RC4 keys": [
    "16dkGStOzdHgjuCciXGdSX7UrHWfYSUG8wEUtKNgzHrWMfTGafJbC",
    "39t3NdDhurvpltFNCpvA5goSylkxjIBtIwWPTv1DPbNEcuIekQC7O"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.345480321.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

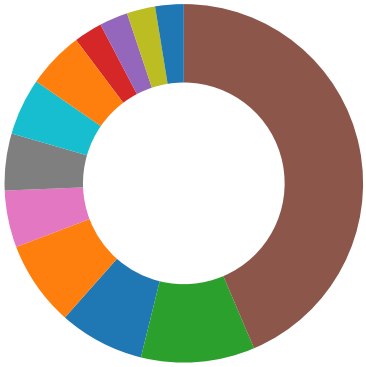
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

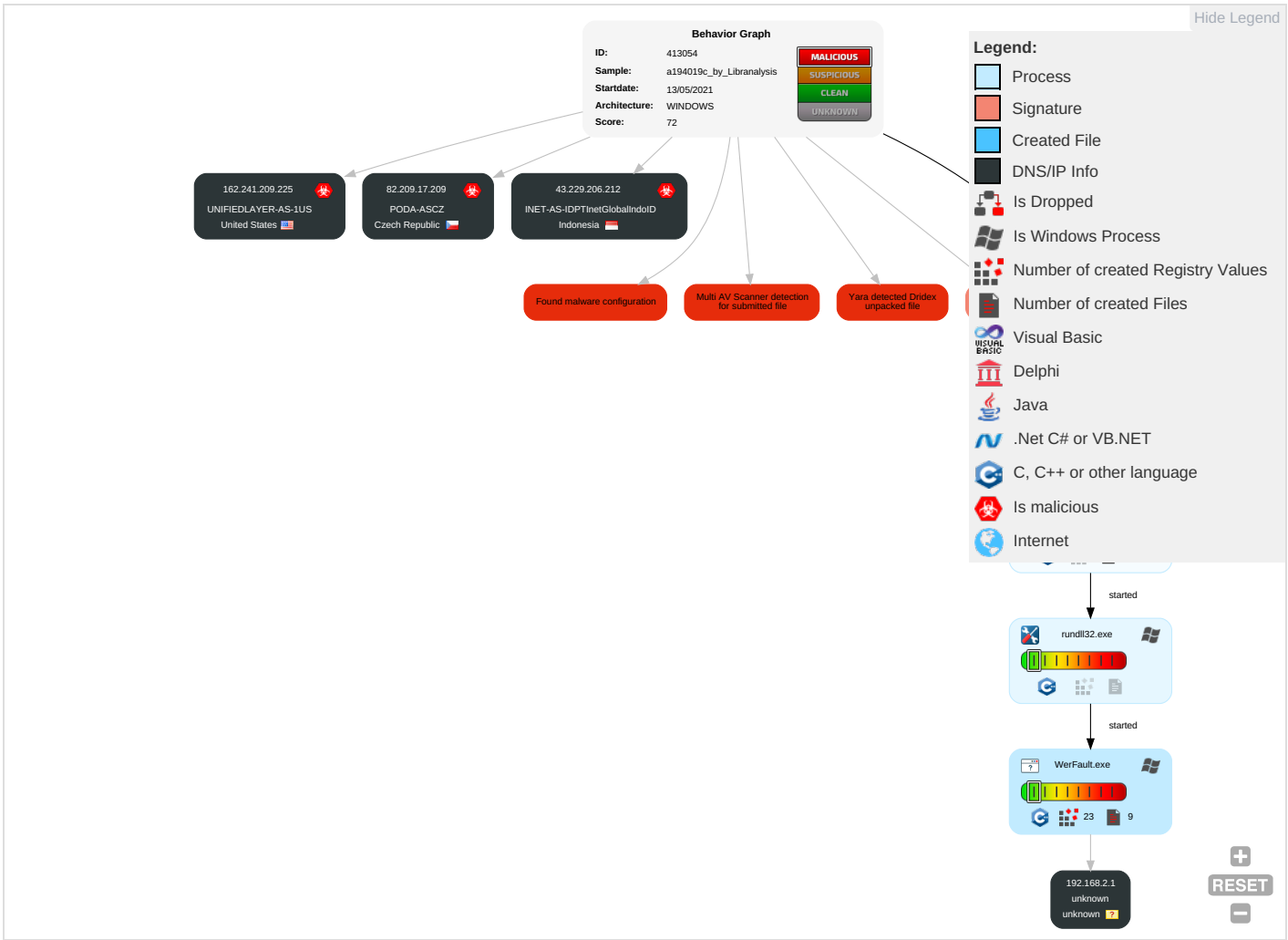
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

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

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

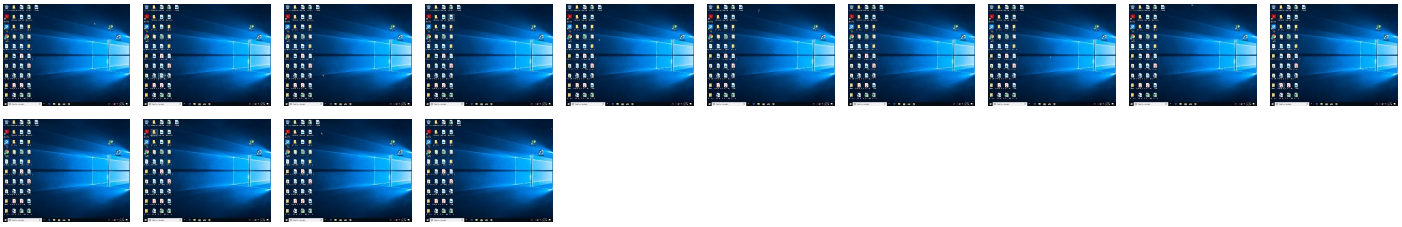
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
a194019c_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
a194019c_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.b40000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

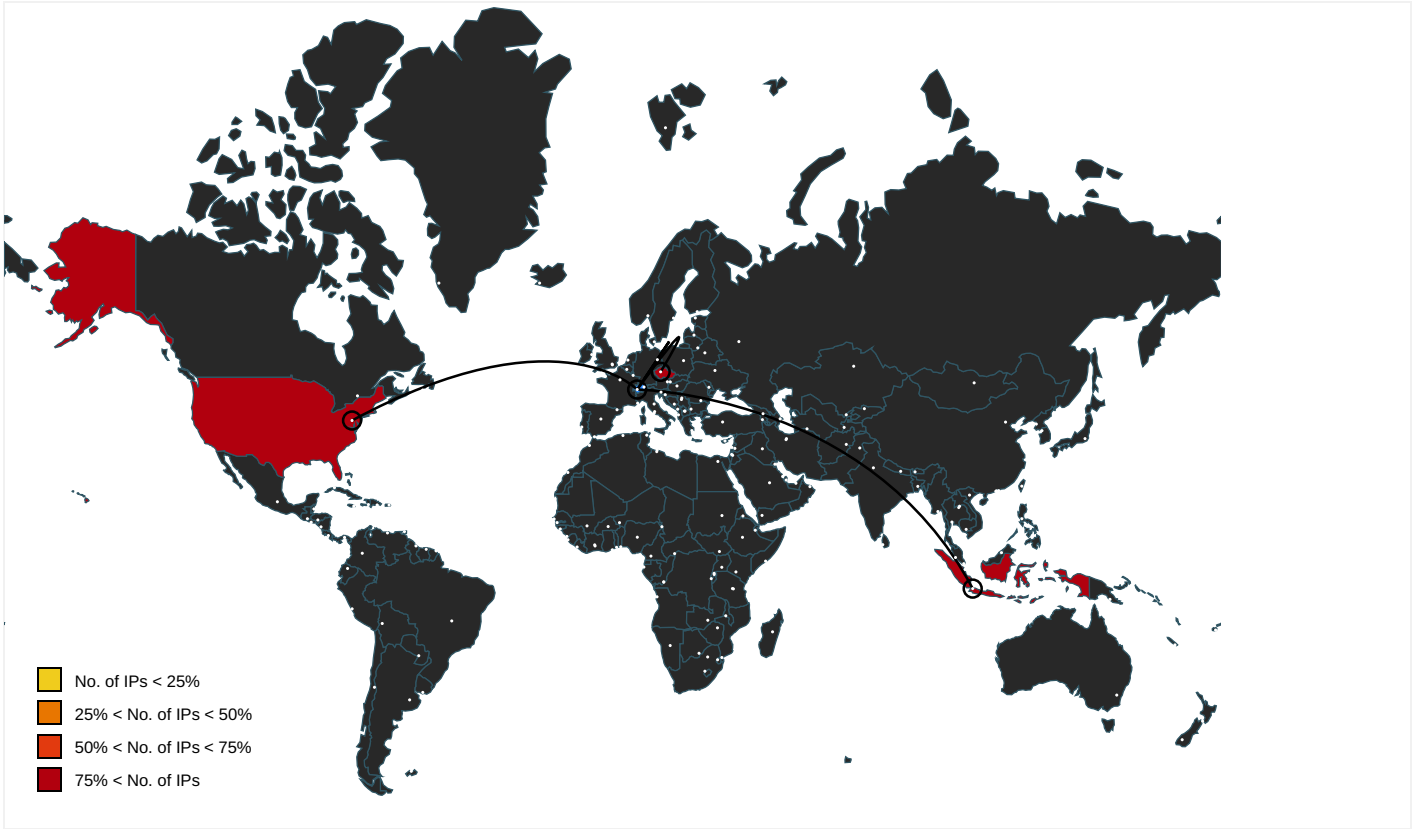
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.micro	WerFault.exe, 0000000E.0000000 3.339585484.0000000004CF8000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413054
Start date:	13.05.2021
Start time:	07:09:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	a194019c_by_Libranalysis (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.winDLL@6/4@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 94.5% (good quality ratio 86.7%) • Quality average: 72.2% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Simulations

Behavior and APIs

Time	Type	Description
07:10:58	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	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	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	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	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
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
UNIFIEDLAYER-AS-1US	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
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0ee1d71e_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_f5ae598134381b1ccff3a8583d69611d275535_82810a17_18c1e370\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12484
Entropy (8bit):	3.76634237091466
Encrypted:	false
SSDEEP:	192:w/7iS0oXccHBUZMX4jed+VG/u7sES274ltWcE:wDi0XXBUZMX4jeh/u7sEX4ltWcE
MD5:	FC05E67DA641B1E80F552A50D9F36883
SHA1:	FC1B6D1C809CF4A432C2BF1D4902282FEACE7190
SHA-256:	72948319518DCA4F0DD890DCB1C2979310C9F9EE5D0F4A1CEA13195DC332E6F9
SHA-512:	54DD92C748FB20A1A4480C1A54C7B2876D6887F066297AA71A3EA2FBD17BCB9BB685A5A7F02F040B1251AE99B89DCA7347F4127458AFC1936916EA89A1EB469

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f5ae598134381b1ccff3a8583d69611d275535_82810a17_18c1e370\Report.wer	
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.=.1.3.2.6.5.3.8.8.6.4.9.3.9.3.0.6.3.6.....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.=.1.3.2.6.5.3.8.8.6.5.6.7.5.2.4.3.5.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.7.8.d.c.6.2.3.-.3.6.0.0.-.4.6.4.5.-.a.2.2.b.-.9.6.d.6.9.2.8.b.2.3.2.e.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.9.d.0.d.3.a.0.-.3.c.4.7.-.4.3.1.9.-.8.8.6.f.-.e.0.5.b.7.9.f.e.9.9.1.1.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.f.8.-.0.0.0.1.-.0.0.1.6.-.4.f.7.d.-.9.d.b.1.0.1.4.8.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\WERC00A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:10:52 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	39326
Entropy (8bit):	2.308039719681678
Encrypted:	false
SSDEEP:	192:Xb7PyGIeBe8TsozJxuHO1UQTsB6ELzc9clFqn80nDI:L7PXlJ8rJxP2zBPLgEFqnD0
MD5:	5CF8AEF622AB621FEBAA60A95029DB30
SHA1:	DAD21813565FA912E8F2867E5831D3D72ADE4866
SHA-256:	09B9C3A4DE07A007084815A35CB5C677D672D2C659640FA2161BBE0EC519DE90
SHA-512:	314DB2ED6EADB2026E1EF339EE76918E26781C66723C9838F88916E6EB5BDD00F89548DBEDD8DB9EDCCEE39942E957CB65235E78F7A967A42A906C663E7DBA86
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....l3.`.....U.....B.....x.....GenuineIntelW.....T.....F3.`.....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\WERCB07.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):	3.6933907278944575
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNitk63R6Yhf6uQgmfT8VSWCprz89bPn1sf0Rlm:RrlsNiO6B6Yp6uQgmfTkSqPnOfX
MD5:	ED426731821471CDAFDA0FD4235EA810
SHA1:	DE4F2FE57C992EA4AE4F7FA9C759FA92653BA093
SHA-256:	B1D43CC55177B2F38E7778953CB2D08651F2BD67B143AEB864C6619D1E779016
SHA-512:	65CB7E55F4E9EE202B66A52C745CC1470E4BFD4AA970C3FA945BF98D8CC45558CF84BF0563C56483816383F783E538331AB1A65EE058125D6B8125089C68DBC
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.3.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD5A.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):	4.470834800709968
Encrypted:	false
SSDEEP:	48:cvIwSD8zsXJgtWI9uIrWSC8BS8fm8M4JCds8NrFuB+q8/hNFa4SrS0d:uITf5hIaSNdJ6NMqNcDW0d
MD5:	23D7C192D0B5C0A63C74ADD66A4F96D8
SHA1:	648232CBA4F1EA6B30DAAC2B563C17A0374184CE
SHA-256:	09AEA6915E4C694B1B7A6A31B8DE50039456008B3FA68057FA4179B2AFB9158D
SHA-512:	967210687EE2A0D2B6DD5B77A51432567FDD8747440E998106379D3B73D78040FD0EC380924BD40E068FAFEA7CFCDC4A8FB5941D695343ADC7B6A9E6BC680FD
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD5A.tmp.xml	
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="987801" />.. <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):	7.513890609445518
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:	a194019c_by_Libranalysis.dll
File size:	167424
MD5:	a194019cde6d134b3e650dc6d4e5d946
SHA1:	e6927771932bc02e1288192f0fd15908a3c30e01
SHA256:	c7b86dcd1d64b9ccb5dda4f0e11bc70cf6e6afcca98cc2cf5c7d6961a4d998ae
SHA512:	39e8dac55667f2089ae5cc737b993bcfcfb40e5828f3f416b8f2ca2aaee28a6132418f829ff5f6f8d2150916b9887d86a0f4da0de79b114391a818ebff05032f
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:	0x609C7F9A [Thu May 13 01:23:38 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 00007F7AD0CBB0B6h
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	0x3ac1	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x99b	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

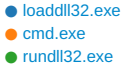
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:10:05.935743093 CEST	65307	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:05.985109091 CEST	53	65307	8.8.8.8	192.168.2.5
May 13, 2021 07:10:06.690767050 CEST	64344	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:10:06.761018991 CEST	53	64344	8.8.8.8	192.168.2.5
May 13, 2021 07:10:07.194355011 CEST	62060	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:07.242979050 CEST	53	62060	8.8.8.8	192.168.2.5
May 13, 2021 07:10:08.303065062 CEST	61805	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:08.353431940 CEST	53	61805	8.8.8.8	192.168.2.5
May 13, 2021 07:10:09.164160967 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:09.212925911 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 07:10:09.665400982 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:09.732558012 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 07:10:10.599474907 CEST	61733	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:10.649416924 CEST	53	61733	8.8.8.8	192.168.2.5
May 13, 2021 07:10:12.194554090 CEST	65447	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:12.254467964 CEST	53	65447	8.8.8.8	192.168.2.5
May 13, 2021 07:10:13.373533010 CEST	52441	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:13.427021980 CEST	53	52441	8.8.8.8	192.168.2.5
May 13, 2021 07:10:14.239994049 CEST	62176	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:14.289212942 CEST	53	62176	8.8.8.8	192.168.2.5
May 13, 2021 07:10:15.365917921 CEST	59596	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:15.414841890 CEST	53	59596	8.8.8.8	192.168.2.5
May 13, 2021 07:10:18.416413069 CEST	65296	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:18.469413996 CEST	53	65296	8.8.8.8	192.168.2.5
May 13, 2021 07:10:20.749978065 CEST	63183	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:20.809817076 CEST	53	63183	8.8.8.8	192.168.2.5
May 13, 2021 07:10:22.101573944 CEST	60151	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:22.161449909 CEST	53	60151	8.8.8.8	192.168.2.5
May 13, 2021 07:10:24.821461916 CEST	56969	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:24.881701946 CEST	53	56969	8.8.8.8	192.168.2.5
May 13, 2021 07:10:58.109299898 CEST	55161	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:58.121260881 CEST	54757	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:58.175317049 CEST	53	55161	8.8.8.8	192.168.2.5
May 13, 2021 07:10:58.181915998 CEST	53	54757	8.8.8.8	192.168.2.5
May 13, 2021 07:10:58.357547045 CEST	49992	53	192.168.2.5	8.8.8.8
May 13, 2021 07:10:58.409281015 CEST	53	49992	8.8.8.8	192.168.2.5
May 13, 2021 07:11:02.005429983 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 07:11:02.057059050 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 07:11:29.677746058 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 07:11:29.750550985 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 07:11:38.222246885 CEST	64345	53	192.168.2.5	8.8.8.8
May 13, 2021 07:11:38.282111883 CEST	53	64345	8.8.8.8	192.168.2.5
May 13, 2021 07:11:54.996006012 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 07:11:55.068980932 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 07:12:04.971366882 CEST	54791	53	192.168.2.5	8.8.8.8
May 13, 2021 07:12:05.028861046 CEST	53	54791	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 800 Parent PID: 5608

General

Start time:	07:10:13
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\a194019c_by_Libranalysis.dll'
Imagebase:	0x2a0000
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: 5700 Parent PID: 800

General

Start time:	07:10:14
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\a194019c_by_Libranalysis.dll',#1
Imagebase:	0xac0000
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: 5368 Parent PID: 5700

General

Start time:	07:10:14
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\a194019c_by_Libranalysis.dll',#1
Imagebase:	0xdc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.345480321.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6288 Parent PID: 5368

General

Start time:	07:10:46
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5368 -s 764
Imagebase:	0xc40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EF01717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EEF497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD5A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD5A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f5ae598134381b1ccff3a8583d69611d275535_82810a17_18c1e370	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f5ae598134381b1ccff3a8583d69611d275535_82810a17_18c1e370\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EEF497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD5A.tmp	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	success or wait	1	6EEF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	success or wait	1	6EEF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD5A.tmp.xml	success or wait	1	6EEF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD77.tmp.csv	success or wait	1	6EEF4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0F3.tmp.txt	success or wait	1	6EEF4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 6c 33 9d 60 a4 05 12 00 00 00 00 00	MDMP..... .....l3.`.....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.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 78 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 f8 14 00 00 46 33 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 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......x..... ..GenuineIntelW...........T... ....F3.`................. ....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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.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 40 35 a1 00 ff ff ff ff ca 30 00 10 19 06 00 02 bc fb 89 00 ca 30 00 10 23 00 00 00 03 02 01 00 38 fb 89 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..#.......8...+.........	success or wait	1	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	168	08 0d 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 ca 30 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 19 06 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 4c 25 00 00	.........................0.... ....L%..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	20	0c 00 00 00 5c fb 47 04 00 00 00 00 a4 04 00 00 74 2e 00 00	....\.G.........t...	success or wait	12	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	1188	bc b1 a2 77 d6 c9 a0 77 64 02 00 00 aa aa aa aa 10 00 00 00 f0 fb 47 04 bc fc 47 04 aa aa aa aa 40 c7 a0 77 40 c7 a0 77 30 07 a1 00 00 c0 62 00 00 c0 62 00 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 c0 62 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 90 07 a2 00 00 00 00 00 00 00 00 00 d0 08 a1 00 00 00 62 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 07 a1 00 00 00 00 00 aa aa aa aa aa aa aa aa 54 02 62 00 54 02 62 00 68 07 a1 00 68 07 a1 00 00 00 00 00 aa aa aa aa 30 07 a1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w...wd.............G...G... ..@..w@..w0.....b...b.....d... ....d.........b............... ....b................. ....0...............T.b.T. b.h...h...........0...........	success or wait	11	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	5316	bc 9a a2 77 a3 1a 32 77 aa aa aa aa 70 ed 89 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 f8 02 00 00 f4 02 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 62 00 00 00 00 00 00 00 00 00 00 00 00 00 70 ed 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w..2w....p.....................................$..b............p...	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	4	02 00 00 00	....	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.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 d0 ec 89 00 bc 9a a2 77 23 00 00 00 12 02 00 00 40 eb 89 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.............w#.......@...+..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	48	2c 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 c0 62 00 00 00 00 00 5c fb 47 04 00 00 00 00 a4 04 00 00 74 2e 00 00 cc 02 00 00 e4 2a 00 00	,....... ....b.....\.G.........t........*..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	752	00 00 05 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 32 25 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 90 11 02 00 00 00 00 00 00 c7 02 00 00 00 00 09 41 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 2c de 00 00 00 00 00 00 39 3d 03 00 00 00 00 00 00 cf 95 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 21 c7 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 1e 00 22 00 00 00 00	...t.....0...U..s@..2%.....B.....B?.....#.....@A.....Zb.....,.....9=.....!.!.....@....."....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t.....F.i.l.e.....F.i.l.e...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.o.C.o.m.p.l.e.t.i.o.n.....T.p.W.o.r.k.e.r.F.a.c.t.o.r.y.....I.R.T.i.m.e.r...(...W.a.i.t.C.o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.....I.R.T.i.m	success or wait	1	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC00A.tmp.dmp	unknown	108	03 00 00 00 64 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 6c 07 00 00 05 00 00 00 c4 00 00 00 b0 2d 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 86 7b 00 00 15 00 00 00 ec 01 00 00 f4 1c 00 00 16 00 00 00 98 00 00 00 e0 1e 00 00	....d.....l.....-.....T.....8.....T.....`....{.....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 33 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.3.6.8.<./.P.i.d.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 38 00 30 00 32 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.>.3.8.0.2.1.<./.U.p.t.i.m.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 36 00 37 00 37 00 35 00 32 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.6.7.7.5.2.9.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 36 00 37 00 36 00 37 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.6.7.6.7.1.0.4.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 31 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.1.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 38 00 33 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.8.3.2.3.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 38 00 33 00 32 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.8.3.2.3.2.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.6.4.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 36 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.6.2.4.<./.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 33 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.>.2.9.3.5.2.<./.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 36 00 35 00 36 00 35 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.6.5.6.5.7.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 36 00 36 00 34 00 37 00 36 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.>.5.6.6.4.7.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 36 00 35 00 36 00 35 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.6.5.6.5.7.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.7.0.0.<./.P.i.d.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0. <./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 38 00 33 00 32 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.8.3.2.9. <./.U.p.t.i.m.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 38 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.>.1.1.2.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 33 00 35 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.3.5.5.5.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.6.3.2.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 35 00 35 00 32 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.5.5.2.0.0.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 36 00 30 00 38 00 35 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.0.8.5.7.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 35 00 35 00 32 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.5.5.2.0.0.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 6e 00 65 00 69 00 6e 00 79 00 64 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.>.n.e.i.n.y.d.,. .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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 6e 00 65 00 69 00 6e 00 79 00 64 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.>.n.e.i.n.y.d.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 37 00 36 00 37 00 32 00 30 00 31 00 30 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.>.1.5.7.6.7.2.0.1.0.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 30 00 3a 00 35 00 32 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.1.4.:.1.0.:.5.2.Z.".>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 33 00 36 00 38 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 37 00 31 00 38 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 37 00 31 00 38 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.=.".3.3.5.". .P.I.D.=.".5.3.6.8.". .U.p.t.i.m.e.M.S.=.".3.0.7.1.8.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".3.0.7.1.8.". .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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 37 00 38 00 64 00 63 00 36 00 32 00 33 00 2d 00 33 00 36 00 30 00 30 00 2d 00 34 00 36 00 34 00 35 00 2d 00 61 00 32 00 32 00 62 00 2d 00 39 00 36 00 64 00 36 00 39 00 32 00 38 00 62 00 32 00 33 00 32 00 65 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.a.7.8.d.c.6.2.3.-.3.6.0.0.-.4.6.4.5.-.a.2.2.b.-.9.6.d.6.9.2.8.b.2.3.2.e.<./.G.u.i.d.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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 30 00 3a 00 35 00 32 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.4.:.1.0.:.5.2.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCB07.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	6EEF497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCD5A.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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f5ae598134381b1ccff3a8583d69611d275535_82810a17_18c1e370\Report.wer	unknown	2	ff fe	..	success or wait	1	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f5ae598134381b1ccff3a8583d69611d275535_82810a17_18c1e370\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	6EEF497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f5ae598134381b1ccff3a8583d69611d275535_82810a17_18c1e370\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 2d 00 36 00 38 00 36 00 31 00 39 00 39 00 33 00 37 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.6.8.6.1.9.9.3.7.9.	success or wait	1	6EEF497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6EF136BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6EF11FB2	RegCreateKeyExW
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EEF43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6EF136BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6EF136BF	unknown
\REGISTRY\A\{2a578781-64a9-f08e-8305-385fdea28d65}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6EF136BF	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	6EF11FE8	RegSetValueExW

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

Disassembly

Code Analysis