ID: 413038
Sample Name:
1c640454_by_Libranalysis
Cookbook: default.jbs
Time: 06:44:33
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

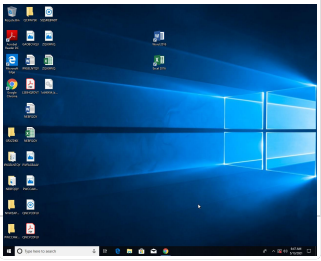
Analysis Report 1c640454_by_Libranalysis

Overview

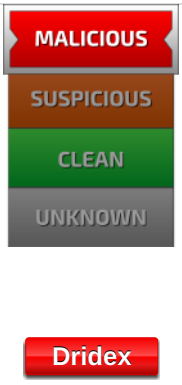
General Information

Sample Name:	1c640454_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	413038
MD5:	1c640454d82c63..
SHA1:	c7603c8cbf7c41a..
SHA256:	610b286c27968d..
Infos:	

Most interesting Screenshot:



Detection



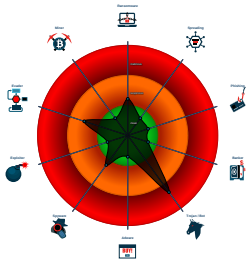
Dridex

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

Signatures

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

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 1404 cmdline: loaddll32.exe 'C:\Users\user\Desktop\1c640454_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4536 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\1c640454_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5056 cmdline: rundll32.exe 'C:\Users\user\Desktop\1c640454_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6864 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5056 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.326422259.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

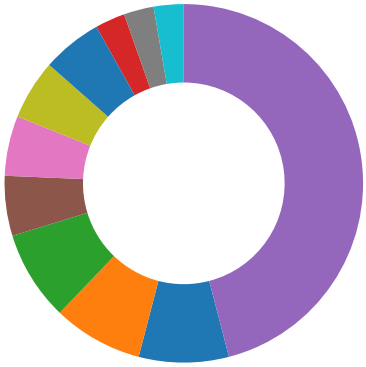
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- 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:

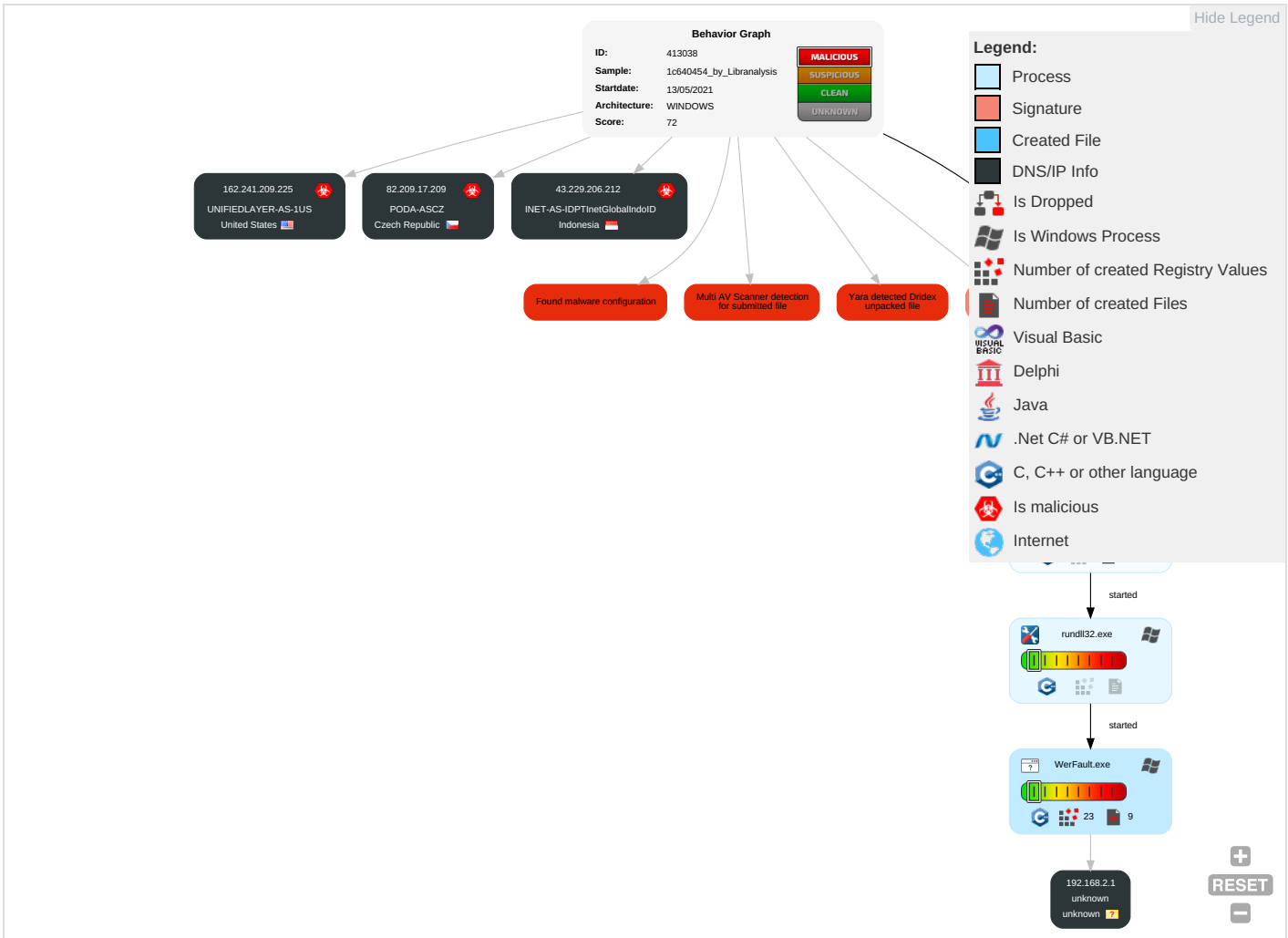
Yara detected Dridex unpacked file

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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1c640454_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
1c640454_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.2790000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

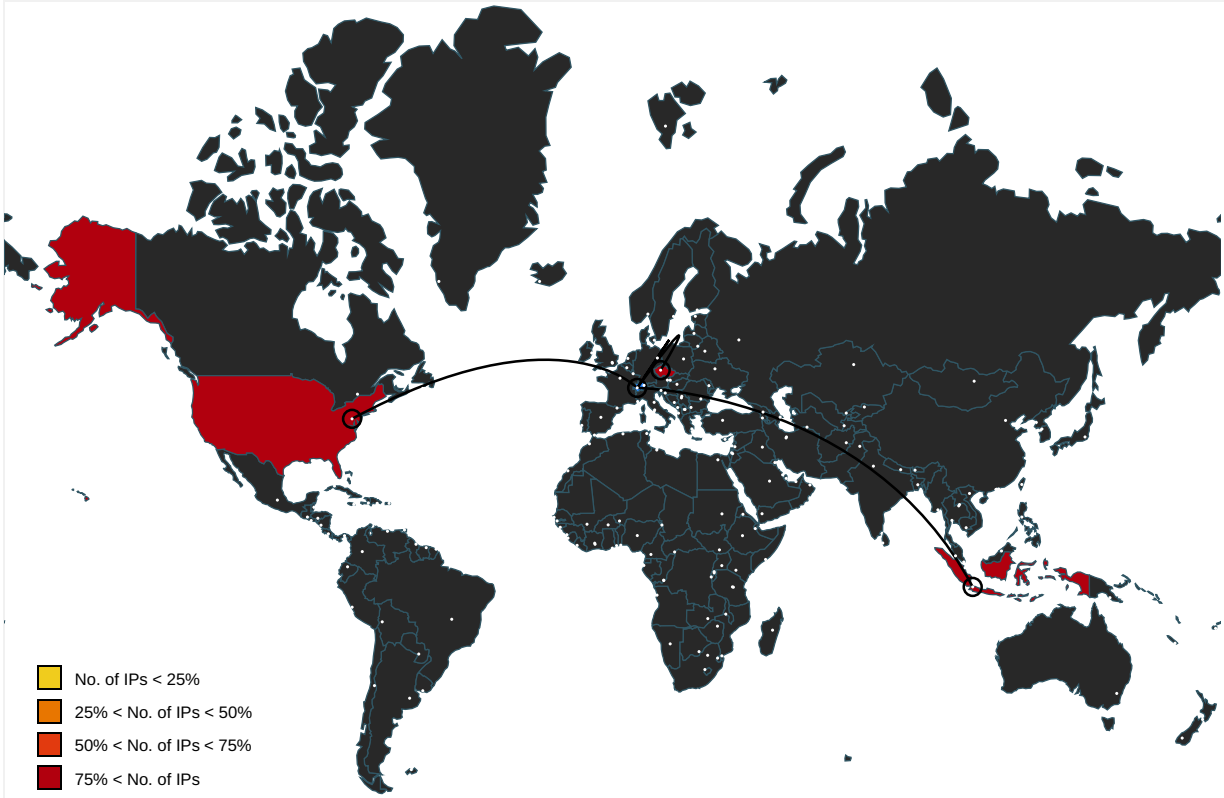
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413038
Start date:	13.05.2021
Start time:	06:44:33

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1c640454_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: 57.2% (good quality ratio 49.4%) • Quality average: 67.2% • Quality standard deviation: 35.7%
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
06:46:06	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	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	1bbde683_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	ce9a5575_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	514b5b51_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	512d531a_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	7c4e952c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	7af9a7b0_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	d310ebba_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_acb49c8a22c31cd0ff11e6b9dc409dfb28af4b20_82810a17_1a9d1575\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12488
Entropy (8bit):	3.766525558216272
Encrypted:	false
SSDEEP:	192:6mi/0oXK4cHBUZMX4jed+3G/u7sZS274ItWcH:riBXKTBUZMX4jeb/u7sZX4ItWcH
MD5:	191005AC8CA5507F0B32B703C0A3F667
SHA1:	DDAA4851D6E68FECD6D5C8040F68D800D1574F40
SHA-256:	51EE7E7184CBDA40A1BA5B97C7CF3D9F416262535489F4993840781397E71533
SHA-512:	6437630263620C6344A2C81202BA985C5EEF2875E4EAB236F627F4086DE38B3CFD5C1D540D10B6D6E133B5FDBF40323A08B1029B4C62B7FEE5AEE716494C8B6
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.=.1.3.2.6.5.3.8.7.1.5.9.1.5.1.6.9.6.6.....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.=.1.3.2.6.5.3.8.7.1.6.5.1.5.1.6.7.7.4.....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.9.d.e.f.5.0.5.-.8.1.2.0.-.4.d.a.2.-.8.d.d.b.-.4.b.5.b.b.b.0.d.9.a.c.1.....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.=.3.a.4.f.4.6.8.a.-.9.e.4.b.-.4.0.f.d.-.b.2.1.5.-.0.3.d.c.1.3.e.5.e.8.d.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.=.0.0.0.0.1.3.c.0.-.0.0.0.1.-.0.0.1.7.-.1.e.6.b.-.c.e.3.9.f.e.4.7.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\WERF7CB.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 13:46:00 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	39238
Entropy (8bit):	2.3419033316564115
Encrypted:	false
SSDEEP:	192:/xFNV5aynXrK5+wLhQnRUHxTq0DW46nlk2bT0liyxnNxS:DNV5amXrK5+4MqkQW46lky0liQu
MD5:	41B22C6920E2ED40DDCCE8404A5BB6EE
SHA1:	ABD63AE5492BE47807BD3CCB7921C59BFB29C196
SHA-256:	D307D9D9111FD670413403D511D3ADDBAFE4BE7C3E262E360F08D478CBB5610F
SHA-512:	8B4FA9408AD4FF0BAB073E2E6FF109FC7E91F932B0B8F607FCD872D9D9C4B9E035092438F2C12D95192222093354CC621A52219D3BDE5F8DE74997AC70E6F07
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....-.`.....U.....B.....x.....GenuineIntelW.....T.....t-.`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....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\WERFD4B.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):	3.698508246109885
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNibt6YJ/6Y326HSgmfT0UVS3Cpr+89b8nlsf0gUm:RrlsNix6+6Ym6HSgmfT0cSI8n+fP
MD5:	E6B482BAC7E9DBDF551002F4383EA0C6
SHA1:	56287714EF877E2301A55C9134DFE86348D1F5B7
SHA-256:	C64BFCB34F9125161D6654910D45E1BDFEF5669CA77BD21041A35AD43C74069F
SHA-512:	1AE9BD42E095819A9135F575DE7E1E55D556EB010368C580406FFF8643C5221BEC58C4FA2617053B4C26EA53339653EF9A270C39703DBC0E06D000CD4810C67A

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	
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.>.5.0.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF9D.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):	4.474690800680671
Encrypted:	false
SSDEEP:	48:cvIwSD8zsStJgtWI9TDWSC8BTU8fm8M4JCdsnNrFN4+q8/iNF74SrST6d:uITfSHoySNrJxNj4BNFDWT6d
MD5:	8DF8D5BAC32B2FBBBB97A5ED5E659234
SHA1:	70281B56303F2F8332AEE40A581908D51344168D
SHA-256:	50E1CF32E5713D27BE916A1A6699C4637AA1893FB036F17F7117F12A7A370A5D
SHA-512:	E9557FEBDFB8F96D753F8AFF523DDE9CC1F151D92DF42BCA1EFC7ECC3783C11E0820EB418A3448852A19C1632210E3AABDCC40A3176651CE05D62B4118B10E ED
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="987776" />.. <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):	7.51388359252741
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:	1c640454_by_Libranalysis.dll
File size:	167424
MD5:	1c640454d82c630e74949cffb0d70e89
SHA1:	c7603c8cbf7c41a5aea125e8030b9c37f81bf285
SHA256:	610b286c27968d72cd8ecd910dbe47ec37d359d60349d2a79a0420595a14ce98
SHA512:	07cee1085f0602e74afaf343f4e853b27d507e99b09048c3a43179133e77033e100c10431012cb7efdef3364836859dcbdad4eb3e871432814c81d391df0a761
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:	0x609C7F8D [Thu May 13 01:23:25 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 00007F1FB07153E6h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2770a	0x5b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x277d8	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x1220	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10018	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x4c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x23dfe	0x23e00	False	0.756362968206	data	7.53078515147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x331c	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x3a0	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x26c	0x400	False	0.548828125	data	4.2946697642	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Version Infos

Description	Data
LegalCopyright	Copyright 2018
InternalName	x2otfb
FileVersion	7.2.5422.00
Full Version	7.2.5_000-b00

Description	Data
CompanyName	Oracle Corporation
ProductName	Xhot(BM) Ltloehey YO 8
ProductVersion	7.2.5422.00
FileDescription	Java(TM) Platform SE binary
OriginalFilename	x2otfb.dll
Translation	0x0000 0x04b0

Network Behavior

UDP Packets

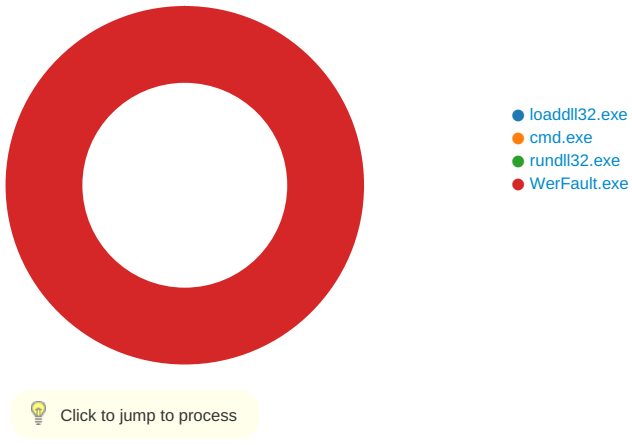
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:45:16.858978033 CEST	62452	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:16.916229963 CEST	53	62452	8.8.8.8	192.168.2.7
May 13, 2021 06:45:16.960442066 CEST	57820	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:17.032674074 CEST	53	57820	8.8.8.8	192.168.2.7
May 13, 2021 06:45:17.078094006 CEST	50848	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:17.126864910 CEST	53	50848	8.8.8.8	192.168.2.7
May 13, 2021 06:45:18.458739996 CEST	61242	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:18.510399103 CEST	53	61242	8.8.8.8	192.168.2.7
May 13, 2021 06:45:19.969510078 CEST	58562	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:20.018170118 CEST	53	58562	8.8.8.8	192.168.2.7
May 13, 2021 06:45:21.363408089 CEST	56590	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:21.413368940 CEST	53	56590	8.8.8.8	192.168.2.7
May 13, 2021 06:45:21.787792921 CEST	60501	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:21.846291065 CEST	53	60501	8.8.8.8	192.168.2.7
May 13, 2021 06:45:22.247548103 CEST	53775	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:22.296412945 CEST	53	53775	8.8.8.8	192.168.2.7
May 13, 2021 06:45:23.401303053 CEST	51837	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:23.452872992 CEST	53	51837	8.8.8.8	192.168.2.7
May 13, 2021 06:45:24.238642931 CEST	55411	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:24.296010017 CEST	53	55411	8.8.8.8	192.168.2.7
May 13, 2021 06:45:25.394905090 CEST	63668	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:25.445341110 CEST	53	63668	8.8.8.8	192.168.2.7
May 13, 2021 06:45:28.848978996 CEST	54640	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:28.900877953 CEST	53	54640	8.8.8.8	192.168.2.7
May 13, 2021 06:45:30.006038904 CEST	58739	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:30.054965019 CEST	53	58739	8.8.8.8	192.168.2.7
May 13, 2021 06:45:31.120771885 CEST	60338	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:31.169487953 CEST	53	60338	8.8.8.8	192.168.2.7
May 13, 2021 06:45:31.901037931 CEST	58717	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:31.951039076 CEST	53	58717	8.8.8.8	192.168.2.7
May 13, 2021 06:45:33.007996082 CEST	59762	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:33.065093994 CEST	53	59762	8.8.8.8	192.168.2.7
May 13, 2021 06:45:34.603598118 CEST	54329	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:34.652767897 CEST	53	54329	8.8.8.8	192.168.2.7
May 13, 2021 06:45:35.820996046 CEST	58052	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:35.873516083 CEST	53	58052	8.8.8.8	192.168.2.7
May 13, 2021 06:45:38.099172115 CEST	54008	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:38.156212091 CEST	53	54008	8.8.8.8	192.168.2.7
May 13, 2021 06:45:42.077595949 CEST	59451	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:42.152453899 CEST	53	59451	8.8.8.8	192.168.2.7
May 13, 2021 06:45:43.340884924 CEST	52914	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:43.389533043 CEST	53	52914	8.8.8.8	192.168.2.7
May 13, 2021 06:45:44.262176037 CEST	64569	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:44.319230080 CEST	53	64569	8.8.8.8	192.168.2.7
May 13, 2021 06:45:45.293451071 CEST	52816	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:45.344130993 CEST	53	52816	8.8.8.8	192.168.2.7
May 13, 2021 06:45:46.928621054 CEST	50781	53	192.168.2.7	8.8.8.8
May 13, 2021 06:45:46.980149984 CEST	53	50781	8.8.8.8	192.168.2.7
May 13, 2021 06:45:47.888087988 CEST	54230	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:45:47.937071085 CEST	53	54230	8.8.8.8	192.168.2.7
May 13, 2021 06:46:05.920085907 CEST	54911	53	192.168.2.7	8.8.8.8
May 13, 2021 06:46:05.977070093 CEST	53	54911	8.8.8.8	192.168.2.7
May 13, 2021 06:46:06.066992044 CEST	49958	53	192.168.2.7	8.8.8.8
May 13, 2021 06:46:06.142282009 CEST	53	49958	8.8.8.8	192.168.2.7
May 13, 2021 06:46:12.870557070 CEST	50860	53	192.168.2.7	8.8.8.8
May 13, 2021 06:46:12.929270983 CEST	53	50860	8.8.8.8	192.168.2.7
May 13, 2021 06:46:26.063349962 CEST	50452	53	192.168.2.7	8.8.8.8
May 13, 2021 06:46:26.131953001 CEST	53	50452	8.8.8.8	192.168.2.7
May 13, 2021 06:46:57.124495029 CEST	59730	53	192.168.2.7	8.8.8.8
May 13, 2021 06:46:57.192188978 CEST	53	59730	8.8.8.8	192.168.2.7
May 13, 2021 06:47:02.482069016 CEST	59310	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:02.541301012 CEST	53	59310	8.8.8.8	192.168.2.7
May 13, 2021 06:47:23.077673912 CEST	51919	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:23.134807110 CEST	53	51919	8.8.8.8	192.168.2.7
May 13, 2021 06:47:23.909102917 CEST	64296	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:23.966233015 CEST	53	64296	8.8.8.8	192.168.2.7
May 13, 2021 06:47:24.566605091 CEST	56680	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:24.624649048 CEST	53	56680	8.8.8.8	192.168.2.7
May 13, 2021 06:47:25.099431038 CEST	58820	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:25.160821915 CEST	53	58820	8.8.8.8	192.168.2.7
May 13, 2021 06:47:25.660111904 CEST	60983	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:25.717369080 CEST	53	60983	8.8.8.8	192.168.2.7
May 13, 2021 06:47:25.756376982 CEST	49247	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:25.815776110 CEST	53	49247	8.8.8.8	192.168.2.7
May 13, 2021 06:47:26.397536039 CEST	52286	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:26.454792023 CEST	53	52286	8.8.8.8	192.168.2.7
May 13, 2021 06:47:26.916636944 CEST	56064	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:26.966615915 CEST	53	56064	8.8.8.8	192.168.2.7
May 13, 2021 06:47:27.819137096 CEST	63744	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:27.881023884 CEST	53	63744	8.8.8.8	192.168.2.7
May 13, 2021 06:47:28.672205925 CEST	61457	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:28.720978975 CEST	53	61457	8.8.8.8	192.168.2.7
May 13, 2021 06:47:29.219227076 CEST	58367	53	192.168.2.7	8.8.8.8
May 13, 2021 06:47:29.270775080 CEST	53	58367	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 1404 Parent PID: 5584

General

Start time:	06:45:24
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\1c640454_by_Libranalysis.dll'
Imagebase:	0x10b0000
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: 4536 Parent PID: 1404

General

Start time:	06:45:24
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\1c640454_by_Libranalysis.dll',#1
Imagebase:	0x870000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5056 Parent PID: 4536

General

Start time:	06:45:24
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\1c640454_by_Libranalysis.dll',#1

Imagebase:	0xf0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.326422259.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6864 Parent PID: 5056

General

Start time:	06:45:57
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5056 -s 764
Imagebase:	0x870000
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	6EAE1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF9D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF9D.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_acb49c8a22c31cd0ff11e6b9dc409dfb28af4b20_82810a17_1a9d1575	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_acb49c8a22c31cd0ff11e6b9dc409dfb28af4b20_82810a17_1a9d1575\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EAD497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF9D.tmp	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	success or wait	1	6EAD4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	success or wait	1	6EAD4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF9D.tmp.xml	success or wait	1	6EAD4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF9B.tmp.csv	success or wait	1	6EAD4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER327.tmp.txt	success or wait	1	6EAD4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 98 2d 9d 60 a4 05 12 00 00 00 00 00	MDMP..... .....-.`.....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.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 c0 13 00 00 74 2d 9d 60 07 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 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 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... .....t-.`..... .....0..=..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.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 c0 36 7c 02 ff ff ff ff ca 30 00 10 19 06 00 02 74 fb 2d 02 ca 30 00 10 23 00 00 00 03 02 01 00 f0 fa 2d 02 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...6|......0......t.- ..0..#.........-.+.........	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	168	b4 15 00 00 00 00 00 00 05 00 00 c0 00 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 cc 02 00 00 4c 25 00 00	.........................0.... ....L%..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	20	0c 00 00 00 fc fb 78 02 00 00 00 00 04 04 00 00 74 2e 00 00	......x.........t...	success or wait	12	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	1028	bc b1 30 77 d6 c9 2e 77 64 02 00 00 aa aa aa aa 10 00 00 00 90 fc 78 02 5c fd 78 02 aa aa aa aa 40 c7 2e 77 40 c7 2e 77 a8 07 7c 02 00 30 58 02 00 30 58 02 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 30 58 02 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa f0 0d 7d 02 00 00 00 00 00 00 00 00 48 09 7c 02 00 a0 57 02 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a8 07 7c 02 00 00 00 00 aa aa aa aa aa aa aa aa 54 a2 57 02 54 a2 57 02 e0 07 7c 02 e0 07 7c 02 00 00 00 00 aa aa aa aa a8 07 7c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..0w...wd............x.\.x... ..@..w@..w..|..0X..0X.....d.. .....d........0X............... ....}... ......H.|...W................. ....|.............T.W.T. W...|...|...........|.........	success or wait	11	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	4096	a8 fd 78 02 00 00 79 02 00 40 78 02 00 00 00 00 00 1e 00 00 00 00 00 00 00 30 58 02 00 00 00 00 c0 13 00 00 54 16 00 00 00 00 00 00 00 00 00 00 00 a0 57 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 29 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	..x...y..@x.............0X... ......T............W......... ....p)w.............	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	4	02 00 00 00	....	success or wait	2	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.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 88 ec 2d 02 bc 9a 30 77 23 00 00 00 02 02 00 00 f8 ea 2d 02 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........- ...0w#.........-.+.........	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	48	54 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 58 02 00 00 00 00 fc fb 78 02 00 00 00 00 04 04 00 00 74 2e 00 00 cc 02 00 00 e4 2a 00 00	T....... ....0X.......x... ......t........*..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.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	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	752	00 00 93 73 00 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 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 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 e0 3e 02 00 00 00 00 00 a0 dc 02 00 00 00 00 ed 4c 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 d0 d9 00 00 00 00 00 00 00 7f 4d 03 00 00 00 00 00 e4 93 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 41 db 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 c5 e9 21 00 00 00 00	...s.....0...U..s@..2%..... .....B.....B?..... .....#..... ..@A.....Zb..... ....>..... .L.....M .....A.!..... @.....!....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t..... .....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(...W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t. .....I.R.T.i.m	success or wait	1	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF7CB.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 2e 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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 30 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.0.5.6.<./.P.i.d.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 35 00 38 00 37 00 30 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.>.3.5.8.7.0.<./.U.p.t.i.m.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 38 00 31 00 39 00 37 00 37 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.>.1.2.7.8.1.9.7.7.6.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 39 00 31 00 34 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.9.1.4.2.4.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 39 00 31 00 34 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.1.9.1.4.2.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 38 00 38 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.6.8.8.8.<./.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.2.9.4.1.6.<./.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 36 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.6.6.8.8.8.6.4.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 39 00 30 00 32 00 33 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.0.2.3.3.6.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 36 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.6.6.8.8.6.4.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 35 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.5.3.6.<./.P.i.d.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0. <./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 31 00 36 00 30 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.>.3.6.1.6.0. <./.U.p.t.i.m.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.4.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 38 00 36 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.9.8.6.8.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.6.3.3.9.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 31 00 36 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.>.3.6.1.6.7.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.6.3.3.9.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 71 00 68 00 79 00 61 00 75 00 78 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.>.q.h.y.a.u.x.,. .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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 71 00 68 00 79 00 61 00 75 00 78 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.>.q.h.y.a.u.x.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 35 00 39 00 33 00 39 00 37 00 33 00 30 00 38 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.>.1.5.5.9.3.9.7.3.0.8.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<.F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./.F.l.a.g.s.>.	success or wait	3	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 34 00 36 00 3a 00 30 00 30 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.1.3.:.4.6.:.0.0.Z.".>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 30 00 35 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 39 00 34 00 39 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 39 00 34 00 39 00 39 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 00	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.3.". .P.I.D.=.".5.0.5.6.". .U.p.t.i.m.e.M.S.=.".2.9.4.9.9.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.9.4.9.9.". .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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 39 00 64 00 65 00 66 00 35 00 30 00 35 00 2d 00 38 00 31 00 32 00 30 00 2d 00 34 00 64 00 61 00 32 00 2d 00 38 00 64 00 64 00 62 00 2d 00 34 00 62 00 35 00 62 00 62 00 62 00 30 00 64 00 39 00 61 00 63 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.a.9.d.e.f.5.0.5.-.8.1.2.0.-.4.d.a.2.-.8.d.d.b.-.4.b.5.b.b.b.0.d.9.a.c.1.<./.G.u.i.d.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 33 00 3a 00 34 00 36 00 3a 00 30 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.3.:.4.6.:.0.0.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD4B.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	6EAD497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFF9D.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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_acb49c8a22c31cd0ff11e6b9dc409dfb28af4b20_82810a17_1a9d1575\Report.wer	unknown	2	ff fe	..	success or wait	1	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_acb49c8a22c31cd0ff11e6b9dc409dfb28af4b20_82810a17_1a9d1575\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	6EAD497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_acb49c8a22c31cd0ff11e6b9dc409dfb28af4b20_82810a17_1a9d1575\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 33 00 30 00 31 00 30 00 36 00 39 00 36 00 33 00 39 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1.3.0.1.0.6.9.6.3.9.	success or wait	1	6EAD497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6EAF36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6EAF1FB2	RegCreateKeyExW
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6EAD43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6EAF36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6EAF36BF	unknown
\REGISTRY\A\{62563d79-f48e-fff7-f6dd-09e27c390eff}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6EAF36BF	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	6EAF1FE8	RegSetValueExW

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

Disassembly

Code Analysis