ID: 413067
Sample Name:
e0eb0cb2_by_Libranalysis.dll
Cookbook: default.jbs
Time: 07:33:06
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

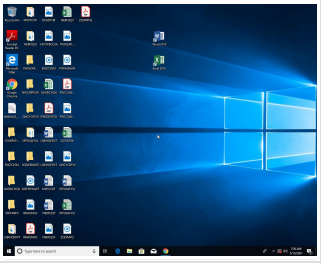
Analysis Report e0eb0cb2_by_Libranalysis.dll

Overview

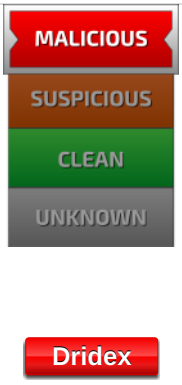
General Information

Sample Name:	e0eb0cb2_by_Libranalysis.dll
Analysis ID:	413067
MD5:	e0eb0cb2de0eef7.
SHA1:	595a9c2ca9bf5b9.
SHA256:	64ee903c9ca580..
Infos:	

Most interesting Screenshot:



Detection

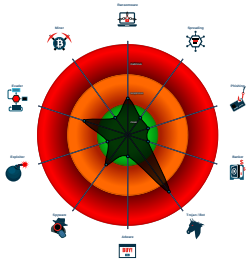


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 3268 cmdline: loaddll32.exe 'C:\Users\user\Desktop\e0eb0cb2_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 3120 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\e0eb0cb2_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5904 cmdline: rundll32.exe 'C:\Users\user\Desktop\e0eb0cb2_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6284 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5904 -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
00000002.00000002.323558475.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

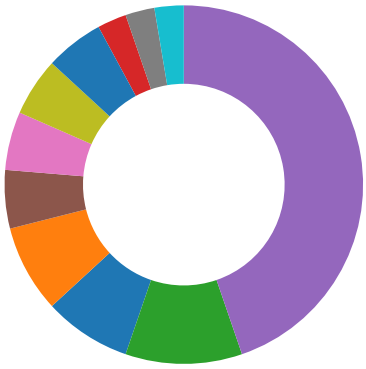
Unpacked PEs

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:

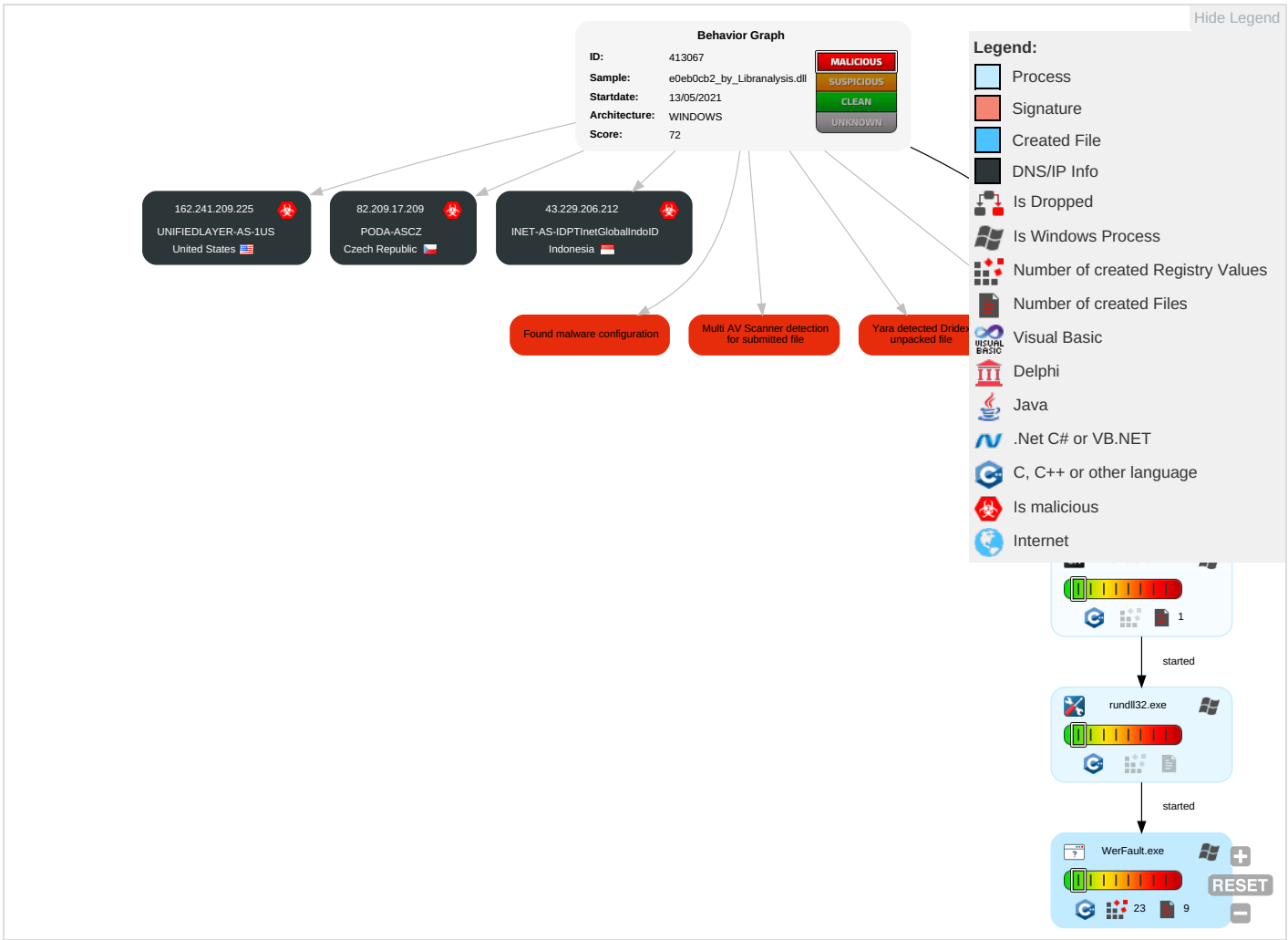
Yara detected Dridex unpacked file

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
e0eb0cb2_by_Libranalysis.dll	38%	ReversingLabs	Win32.Trojan.Convagent	
e0eb0cb2_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.a60000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

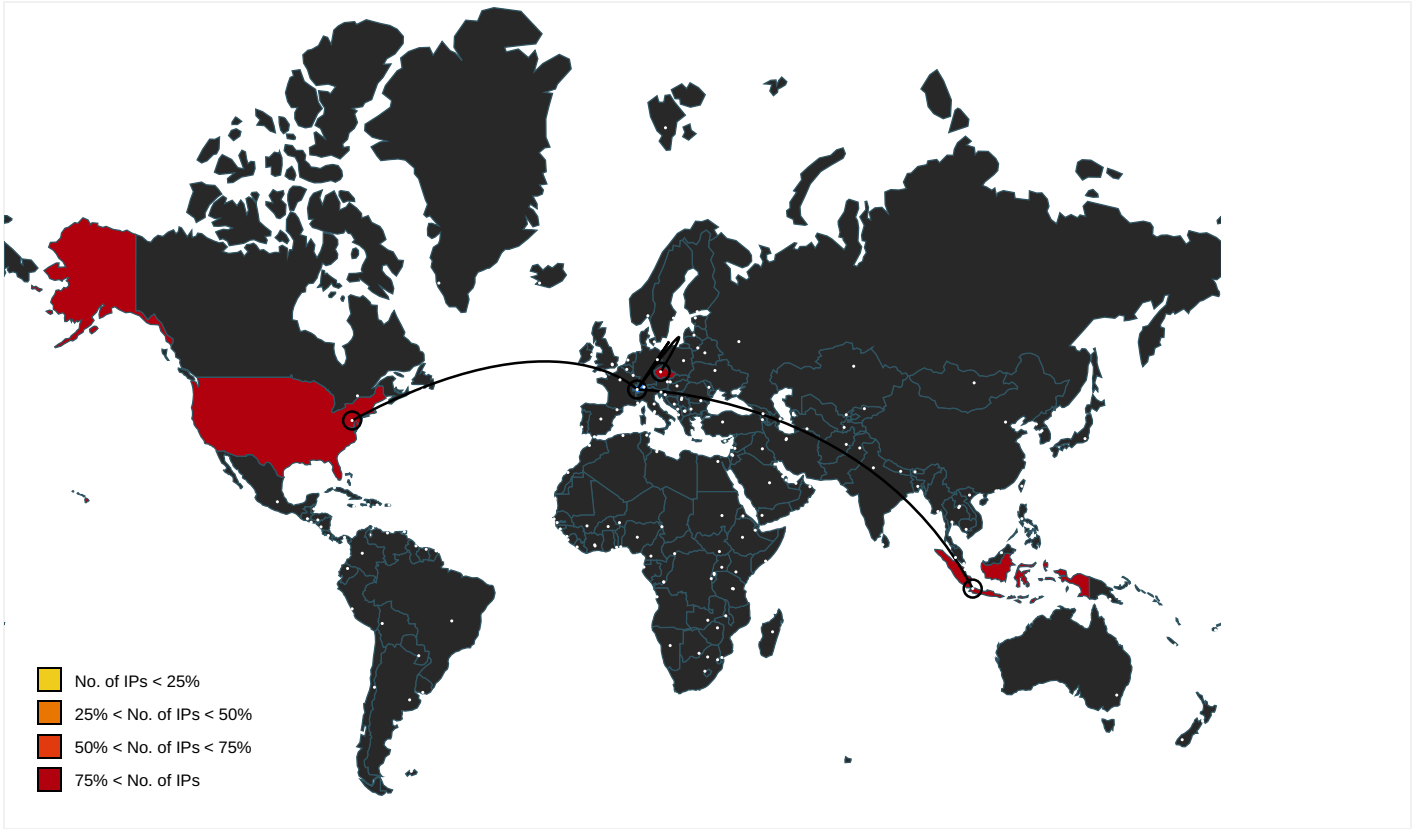
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.m	WerFault.exe, 0000000F.0000000 3.317823061.0000000005021000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413067
Start date:	13.05.2021
Start time:	07:33:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	e0eb0cb2_by_Libranalysis.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 94.3% (good quality ratio 86.5%) • Quality average: 72.1% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	04f506ab_by_Libranalysis.dll	Get hash	malicious	Browse	
	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	04f506ab_by_Libranalysis.dll	Get hash	malicious	Browse	
	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	
	04f506ab_by_Libranalysis.dll	Get hash	malicious	Browse	
	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	04f506ab_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	04f506ab_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	04f506ab_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	bba45991_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_cd85591aac192fb49deadb9cb5ae67e30113580_82810a17_18c57ae9\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12454
Entropy (8bit):	3.7659466038560763
Encrypted:	false
SSDEEP:	192:ZlBi80oXzcHBUZMX4jed+jG/u7seS274ItWcI:1iaXwBUZMX4jeP/u7seX4ItWcI
MD5:	4E54281B5885104C03A4BA58878BACD4
SHA1:	AF7D1A02BC5C013443E05D4CAE88D20B0BC47B58
SHA-256:	E0BC719F5EFEDF79C7CDBCC3AC813CD0BE565CC986076B22725F000FA525F25E
SHA-512:	BED4F0A4A9BF402BD93C6D8530E30FAC26F0C19B5849EAEE6F69A9AF0FD2375518F644FA7E82D3E3EC34F853D6D801C6686FA6E1339551BFDB137825E650525
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.9.0.0.6.8.9.9.6.0.2.8.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.9.0.0.7.6.8.8.6.6.2.9.6.....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.=.2.0.0.c.1.2.1.b.-.5.7.d.6.-.4.c.4.c.-.b.6.0.9.-.a.4.1.f.2.6.5.c.4.6.e.3.....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.=.a.d.a.8.b.0.9.c.-.a.8.5.e.-.4.5.0.7.-.9.5.e.2.-.1.a.8.9.6.6.e.7.c.4.0.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.1.0.-.0.0.0.1.-.0.0.1.7.-.d.0.f.5.-.5.8.0.2.0.5.4.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:34:30 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	54834
Entropy (8bit):	1.9268053243791279
Encrypted:	false
SSDEEP:	192:A9ipTCRjjTauQypLpjcGfzjuBjs1Z3kDxIjPb7rnWnq:Kil2fJbp9j2lsDUDejPbvN
MD5:	402333E81F1223444A7581FE3AE9CAEA
SHA1:	A17ACDB51A96AC4E2588BEB39EB5EF4367B84678
SHA-256:	6B06A5FDAC8D06495A2508F36DF81FE4A133CA3E29B3040FC44C9010582815A6
SHA-512:	76405F9AC562B37453F8DB3D4A1F0FCD95E47F80931B6CB1F5AE281D472E997AE143EF2AFD9FA49C9218C943250AB06C3EDA3E22CDB1224CE013211E0BBEF59
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....8.`.....U.....B.....GenuineIntelW.....T.....8.`.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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):	3.6930927151828854
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipgMn6jg6Yj168BfEgmfTDVSENCpr189bknjsfrMm:RrlsNipz6E6YR6SsgmfTpSEXknIfV
MD5:	2F80AA51CA7DBEA4022B782644705A78
SHA1:	D7FCC8853CED3AAA183B8E5D9BC22B48776E77AB
SHA-256:	458B7B2B434CCFB15C04D89614EA6F359FCC30BDD218E430955F84310B181549
SHA-512:	4592F224022E160D7409A9879CE106E5B48DE956D6A4368A729CF42F6A5B0DB654A3D64D8C982F17715D6C8F7E920F423C007FB13E32B3BE4AE6C28EE71EE9E
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.0.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E3C.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):	4.4694186593077685
Encrypted:	false
SSDEEP:	48:cvIwSD8zsJJgtWI9fXWSC8Bd7B8fm8M4JCdsLNrF4v9g+q8/eNFJy4SrST6d:uITfbYmSNrGJNNM9gdN/yDWT6d
MD5:	055BDE406D94AA6A6E228AD2E703263A
SHA1:	D71BE3E7ABA0D6CE3D4319CD3554E5BD1CBB3935
SHA-256:	0617FDE32637D39AA7FFE98E589ED76D1A96A56010EFFDB9C9121F8ADD7C1EE4
SHA-512:	C3BDBF1C5F3931D542E550CC65ED172A59CAC64F014628E28D6DFA80BE2D55E0BCDE3FB4A267832E57F91244B2EF188FD565FB543109E45E76AD87B0D6FDC16
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="987825" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.513865815249202
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:	e0eb0cb2_by_Libranalysis.dll
File size:	167424
MD5:	e0eb0cb2de0eef7b7e755cb5f27f6725
SHA1:	595a9c2ca9bf5b9781d070b51a8cb8b2d4273803
SHA256:	64ee903c9ca580a02bcdb5c15c785e4e4a737e09a6c0b9e86709887424b379fc
SHA512:	6c090af9d33d4cb92a6d6ef6bc5c239f9a600fdf404f9aa0a9b170fafa617877f01b258d4eb61dc2fc12841e36a0432d5e5a0b6987a4b8f46fcd21762143150b
SSDEEP:	3072:79F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:79F6rQXvFczvYpQP

General

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:	0x609C8026 [Thu May 13 01:25:58 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 00007F9820E32456h
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

Instruction
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

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	0x23e44	0x23e00	False	0.756362968206	data	7.53078515147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x34d0	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x3a0	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x26c	0x400	False	0.548828125	data	4.2946697642	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Version Infos

Description	Data
LegalCopyright	Copyright 2018
InternalName	x2otfb
FileVersion	7.2.5422.00
Full Version	7.2.5_000-b00
CompanyName	Oracle Corporation
ProductName	Xhot(BM) Ltloehey YO 8
ProductVersion	7.2.5422.00
FileDescription	Java(TM) Platform SE binary
OriginalFilename	x2otfb.dll
Translation	0x0000 0x04b0

Network Behavior

UDP Packets

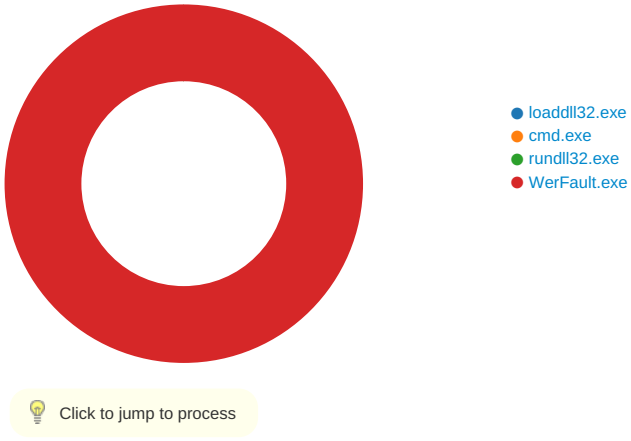
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:33:49.466989994 CEST	53	62452	8.8.8.8	192.168.2.7
May 13, 2021 07:33:49.494098902 CEST	57820	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:49.553380013 CEST	53	57820	8.8.8.8	192.168.2.7
May 13, 2021 07:33:50.237241983 CEST	50848	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:50.285927057 CEST	53	50848	8.8.8.8	192.168.2.7
May 13, 2021 07:33:51.539207935 CEST	61242	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:51.590888023 CEST	53	61242	8.8.8.8	192.168.2.7
May 13, 2021 07:33:52.306633949 CEST	58562	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:52.363642931 CEST	53	58562	8.8.8.8	192.168.2.7
May 13, 2021 07:33:52.507565022 CEST	56590	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:52.556361914 CEST	53	56590	8.8.8.8	192.168.2.7
May 13, 2021 07:33:53.689897060 CEST	60501	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:53.740179062 CEST	53	60501	8.8.8.8	192.168.2.7
May 13, 2021 07:33:55.372215033 CEST	53775	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:55.422761917 CEST	53	53775	8.8.8.8	192.168.2.7
May 13, 2021 07:33:56.340138912 CEST	51837	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:56.391830921 CEST	53	51837	8.8.8.8	192.168.2.7
May 13, 2021 07:33:57.357034922 CEST	55411	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:57.408510923 CEST	53	55411	8.8.8.8	192.168.2.7
May 13, 2021 07:33:58.434393883 CEST	63668	53	192.168.2.7	8.8.8.8
May 13, 2021 07:33:58.483097076 CEST	53	63668	8.8.8.8	192.168.2.7
May 13, 2021 07:34:01.273425102 CEST	54640	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:01.325109005 CEST	53	54640	8.8.8.8	192.168.2.7
May 13, 2021 07:34:03.063937902 CEST	58739	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:03.112528086 CEST	53	58739	8.8.8.8	192.168.2.7
May 13, 2021 07:34:08.267966032 CEST	60338	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:08.316772938 CEST	53	60338	8.8.8.8	192.168.2.7
May 13, 2021 07:34:09.305231094 CEST	58717	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:09.354592085 CEST	53	58717	8.8.8.8	192.168.2.7
May 13, 2021 07:34:10.232156038 CEST	59762	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:10.289232969 CEST	53	59762	8.8.8.8	192.168.2.7
May 13, 2021 07:34:11.908926010 CEST	54329	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:11.957659006 CEST	53	54329	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:34:16.427026987 CEST	58052	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:16.479141951 CEST	53	58052	8.8.8.8	192.168.2.7
May 13, 2021 07:34:17.332051039 CEST	54008	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:17.380858898 CEST	53	54008	8.8.8.8	192.168.2.7
May 13, 2021 07:34:18.441901922 CEST	59451	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:18.499435902 CEST	53	59451	8.8.8.8	192.168.2.7
May 13, 2021 07:34:18.993828058 CEST	52914	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:19.059504032 CEST	53	52914	8.8.8.8	192.168.2.7
May 13, 2021 07:34:19.940792084 CEST	64569	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:19.989517927 CEST	53	64569	8.8.8.8	192.168.2.7
May 13, 2021 07:34:20.809715986 CEST	52816	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:20.858880997 CEST	53	52816	8.8.8.8	192.168.2.7
May 13, 2021 07:34:22.060661077 CEST	50781	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:22.120985985 CEST	53	50781	8.8.8.8	192.168.2.7
May 13, 2021 07:34:23.101773977 CEST	54230	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:23.150592089 CEST	53	54230	8.8.8.8	192.168.2.7
May 13, 2021 07:34:36.233150959 CEST	54911	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:36.290636063 CEST	53	54911	8.8.8.8	192.168.2.7
May 13, 2021 07:34:38.140355110 CEST	49958	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:38.189169884 CEST	53	49958	8.8.8.8	192.168.2.7
May 13, 2021 07:34:44.701622963 CEST	50860	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:44.750334978 CEST	53	50860	8.8.8.8	192.168.2.7
May 13, 2021 07:34:52.605473042 CEST	50452	53	192.168.2.7	8.8.8.8
May 13, 2021 07:34:52.663793087 CEST	53	50452	8.8.8.8	192.168.2.7
May 13, 2021 07:35:21.050159931 CEST	59730	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:21.107441902 CEST	53	59730	8.8.8.8	192.168.2.7
May 13, 2021 07:35:26.701179028 CEST	59310	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:26.759025097 CEST	53	59310	8.8.8.8	192.168.2.7
May 13, 2021 07:35:41.700639009 CEST	51919	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:41.757919073 CEST	53	51919	8.8.8.8	192.168.2.7
May 13, 2021 07:35:42.353214025 CEST	64296	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:42.402101994 CEST	53	64296	8.8.8.8	192.168.2.7
May 13, 2021 07:35:42.969805956 CEST	56680	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:43.026997089 CEST	53	56680	8.8.8.8	192.168.2.7
May 13, 2021 07:35:43.107856989 CEST	58820	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:43.170133114 CEST	53	58820	8.8.8.8	192.168.2.7
May 13, 2021 07:35:43.478653908 CEST	60983	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:43.527333021 CEST	53	60983	8.8.8.8	192.168.2.7
May 13, 2021 07:35:44.066730022 CEST	49247	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:44.123954058 CEST	53	49247	8.8.8.8	192.168.2.7
May 13, 2021 07:35:44.670387983 CEST	52286	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:44.719119072 CEST	53	52286	8.8.8.8	192.168.2.7
May 13, 2021 07:35:45.314290047 CEST	56064	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:45.363136053 CEST	53	56064	8.8.8.8	192.168.2.7
May 13, 2021 07:35:46.161200047 CEST	63744	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:46.222512007 CEST	53	63744	8.8.8.8	192.168.2.7
May 13, 2021 07:35:47.377065897 CEST	61457	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:47.434437990 CEST	53	61457	8.8.8.8	192.168.2.7
May 13, 2021 07:35:48.039921045 CEST	58367	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:48.100116014 CEST	53	58367	8.8.8.8	192.168.2.7
May 13, 2021 07:35:57.815222025 CEST	60599	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:57.874515057 CEST	53	60599	8.8.8.8	192.168.2.7
May 13, 2021 07:35:59.353189945 CEST	59571	53	192.168.2.7	8.8.8.8
May 13, 2021 07:35:59.410504103 CEST	53	59571	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 3268 Parent PID: 5768

General

Start time:	07:33:57
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\e0eb0cb2_by_Libranalysis.dll'
Imagebase:	0xa00000
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: 3120 Parent PID: 3268

General

Start time:	07:33:57
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\e0eb0cb2_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: 5904 Parent PID: 3120

General

Start time:	07:33:58
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\e0eb0cb2_by_Libranalysis.dll',#1
Imagebase:	0xaa0000
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: 00000002.00000002.323558475.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6284 Parent PID: 5904

General

Start time:	07:34:26
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5904 -s 764
Imagebase:	0x1080000
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	6D281717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D27497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E3C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E3C.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_cd85591aac192fb49deadb9cb5ae67e30113580_82810a17_18c57ae9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_cd85591aac192fb49deadb9cb5ae67e30113580_82810a17_18c57ae9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D27497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E3C.tmp	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	success or wait	1	6D274BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	success or wait	1	6D274BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E3C.tmp.xml	success or wait	1	6D274BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E3A.tmp.csv	success or wait	1	6D274BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66A7.tmp.txt	success or wait	1	6D274BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 f6 38 9d 60 a4 05 12 00 00 00 00 00	MDMP..... .....8.`.....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.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 d8 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 10 17 00 00 d6 38 9d 60 07 00 00 00 11 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	.....U...........B............ ..GenuineIntelW...........T... ....8.`.................. ....0..=............... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e................... ....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e..........	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.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 77 00 ff ff ff ff ca 30 00 10 19 06 00 02 ec f6 63 00 ca 30 00 10 23 00 00 00 03 02 01 00 68 f6 63 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	....+...S...+. ..+........0...6w......0...... ..c..0..#.......h.c.+.........	success or wait	1	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	168	4c 15 00 00 00 00 00 00 05 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 ca 30 00 10 00 00 00 00 02 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 19 06 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 cc 02 00 00 ac 25 00 00	L........................0.... ....%..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	20	11 00 00 00 98 c9 76 00 00 00 00 00 04 00 00 00 bc 34 00 00	......v..........4..	success or wait	17	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	4	dc f6 95 00	....	success or wait	16	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	832	bc b1 30 77 d6 c9 2e 77 64 02 00 00 aa aa aa aa 10 00 00 00 54 fd a5 00 20 fe a5 00 aa aa aa aa 40 c7 2e 77 40 c7 2e 77 aa aa aa aa 00 f0 5a 00 00 f0 5a 00 00 00 00 00 64 02 00 00 aa aa aa aa 64 02 00 00 aa aa aa aa 00 f0 5a 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 40 18 78 00 00 00 00 00 00 00 00 00 48 09 77 00 00 30 5a 00 10 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 aa aa aa aa aa aa aa aa 54 32 5a 00 e0 f7 9d 00 e0 07 77 00 e8 f7 9d 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	..0w...wd...........T... ....@..w@..w......Z...Z.....d... ....d.........Z.............. ....@.x... ......H.w..0Z................ ....T2Z... ....w........................	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.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 00 e8 63 00 bc 9a 30 77 23 00 00 00 12 02 00 00 70 e6 63 00 2b 00 00 00 aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa	?............................ ....+...S...+. ..+....................0...... ..c...0w#.......p.c.+.........	success or wait	4	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	48	18 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 f0 5a 00 00 00 00 00 c0 fc a5 00 00 00 00 00 40 03 00 00 d8 a8 00 00 cc 02 00 00 dc 30 00 00	....Z........... ..@............0..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.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	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	752	00 00 93 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 92 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 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 b0 47 02 00 00 00 00 00 b0 e1 02 00 00 00 00 9e 4b 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 e0 d7 00 00 00 00 00 00 00 a4 51 03 00 00 00 00 00 cd a1 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 e9 ff 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 09 13 22 00 00 00 00	...s.....0...U..s@...%..... .....B.....B?..... .....#..... ..@A.....Zb..... ....G..... .K.....Q .....!..... @....."....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.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	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER52DF.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 cc 07 00 00 05 00 00 00 14 01 00 00 a8 33 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 1a b8 00 00 15 00 00 00 ec 01 00 00 54 1d 00 00 16 00 00 00 98 00 00 00 40 1f 00 00	....3.....T.....8.....T.....`.....T.....@...	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.9.0.4.<./.P.i.d.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 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	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 32 00 38 00 37 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.2.8.7.5.<./.U.p.t.i.m.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 32 00 33 00 38 00 37 00 32 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.>.1.2.7.8.2.3.8.7.2.<./.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 38 00 31 00 35 00 36 00 38 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.8.1.5.6.8.0.<./.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 39 00 37 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.6.9.7.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 34 00 30 00 35 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.4.0.5.7.6.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 34 00 30 00 35 00 37 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.4.0.5.7.6.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.4.1.6.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.0.7.7.6.<./.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 33 00 30 00 35 00 30 00 34 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.>.3.0.5.0.4.<./.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 39 00 31 00 30 00 35 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.1.0.5.2.8.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 31 00 38 00 37 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.1.8.7.2.0.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 39 00 31 00 30 00 35 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.9.1.0.5.2.8.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 32 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.3.1.2.0.<./.P.i.d.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 33 00 33 00 36 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.3.3.6.4. <./.U.p.t.i.m.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 30 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.>.1.1.2.0.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 31 00 39 00 31 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.1.9.1.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 38 00 32 00 33 00 30 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.>.3.6.8.2.3.0.4.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 32 00 32 00 34 00 33 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.>.2.3.2.2.4.3.2.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 39 00 39 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.7.9.9.0.4.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 32 00 32 00 34 00 33 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.>.2.3.2.2.4.3.2.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 69 00 63 00 67 00 74 00 61 00 68 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.>.i.c.g.t.a.h.,. .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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 69 00 63 00 67 00 74 00 61 00 68 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.>.i.c.g.t.a.h.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 38 00 35 00 30 00 39 00 37 00 36 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.5.9.8.5.0.9.7.6.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 33 00 34 00 3a 00 33 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.=.".2.0.2.1.-.0.5.-.1.3.T.1.4.:.3.4.:.3.1.Z.".>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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 39 00 30 00 34 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 37 00 36 00 34 00 30 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 37 00 36 00 34 00 30 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.3.". .P.I.D.=.".5.9.0.4.". .U.p.t.i.m.e.M.S.=.".2.7.6.4.0.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.7.6.4.0.". .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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 32 00 30 00 30 00 63 00 31 00 32 00 31 00 62 00 2d 00 35 00 37 00 64 00 36 00 2d 00 34 00 63 00 34 00 63 00 2d 00 62 00 36 00 30 00 39 00 2d 00 61 00 34 00 31 00 66 00 32 00 36 00 35 00 63 00 34 00 36 00 65 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.2.0.0.c.1.2.1.b.-.5.7.d.6.-.4.c.4.c.-.b.6.0.9.-.a.4.1.f.2.6.5.c.4.6.e.3.<./.G.u.i.d.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 33 00 34 00 3a 00 33 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.4.:.3.4.:.3.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5AB0.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	6D27497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E3C.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	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_cd85591aac192fb49deadb9cb5ae67e30113580_82810a17_18c57ae9\Report.wer	unknown	2	ff fe	..	success or wait	1	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_cd85591aac192fb49deadb9cb5ae67e30113580_82810a17_18c57ae9\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	181	6D27497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_cd85591aac192fb49deadb9cb5ae67e30113580_82810a17_18c57ae9\Report.wer	unknown	44	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 38 00 31 00 31 00 39 00 32 00 30 00 31 00 34 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.8.1.1.9.2.0.1.4.3.	success or wait	1	6D27497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D2936BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D291FB2	RegCreateKeyExW
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2743D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D2936BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D2936BF	unknown
\REGISTRY\A\{dae5e2ba-78eb-6112-5e24-9a556f5d4449}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D2936BF	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	6D291FE8	RegSetValueExW

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

Disassembly

Code Analysis