ID: 413052
Sample Name:
86fa0c16_by_Libranalysis
Cookbook: default.jbs
Time: 07:06:01
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

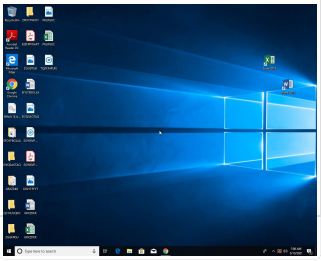
Analysis Report 86fa0c16_by_Libranalysis

Overview

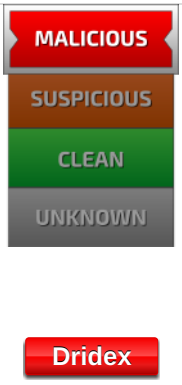
General Information

Sample Name:	86fa0c16_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	413052
MD5:	86fa0c1657be46e.
SHA1:	d5a06060a0b052..
SHA256:	e766f64fbc9a86d..
Infos:	

Most interesting Screenshot:



Detection

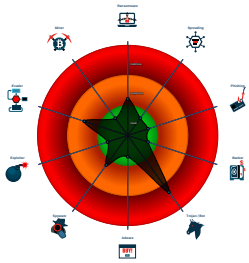


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 2316 cmdline: loaddll32.exe 'C:\Users\user\Desktop\86fa0c16_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 1544 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\86fa0c16_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2964 cmdline: rundll32.exe 'C:\Users\user\Desktop\86fa0c16_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6800 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2964 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22202,
  "C2 list": [
    "43.229.206.212:443",
    "82.209.17.209:8172",
    "162.241.209.225:4125"
  ],
  "RC4 keys": [
    "16dkGStOzdHgjuCciXGdSX7UrHWfYSUG8wEUtKNgzHrWMfTGafJbC",
    "UlufoCqJDohDzGOdBY6ldd1IbFW5KV8BqCAnkqwdDzvq0CsZOOngL"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.317136592.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

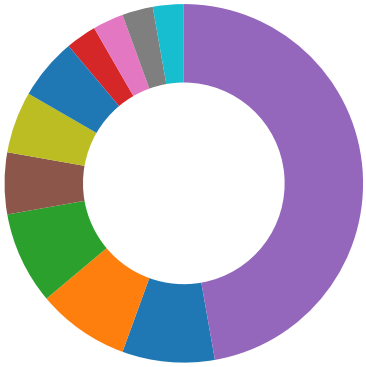
Unpacked PEs

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:

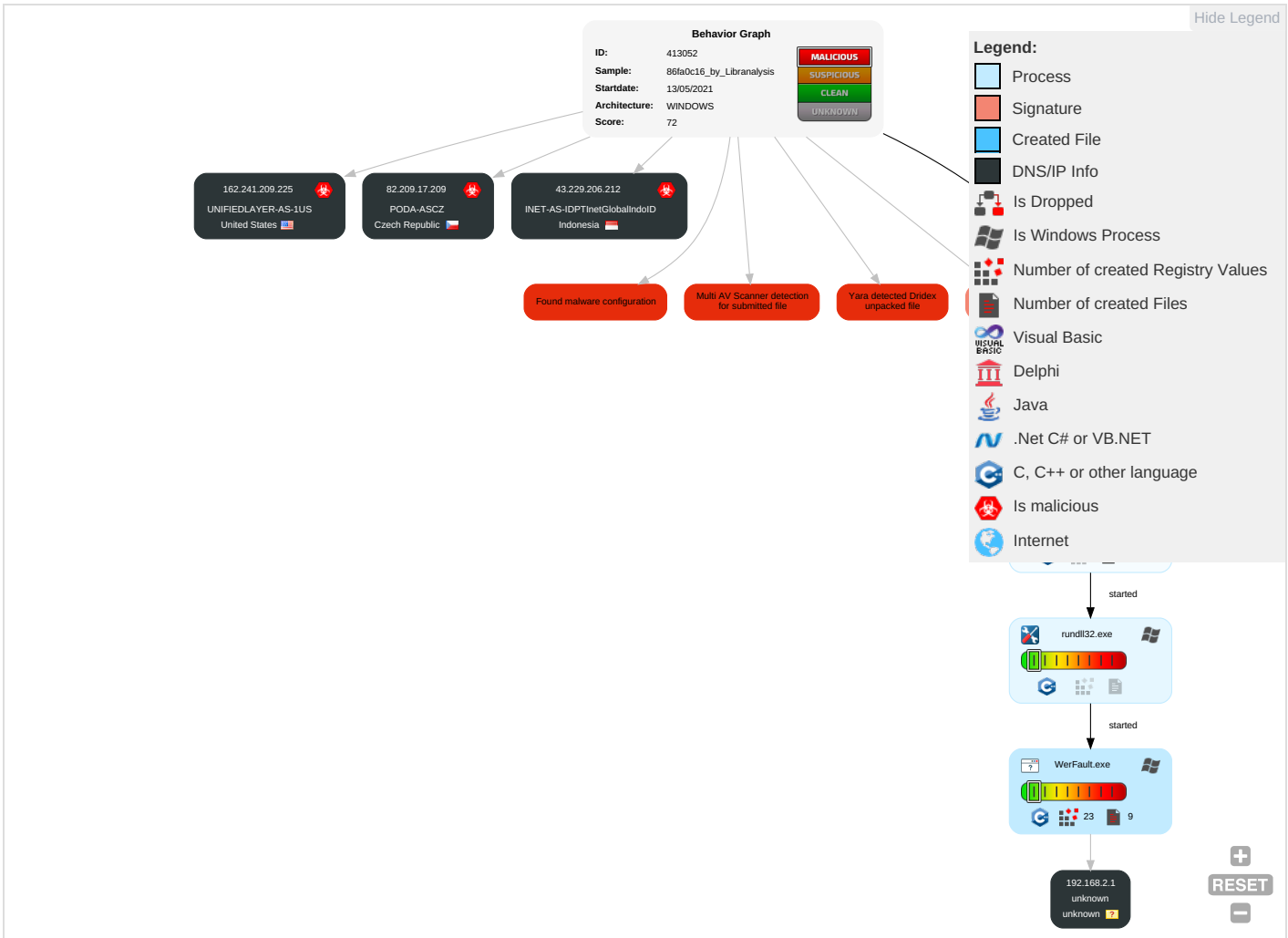
Yara detected Dridex unpacked file

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	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on 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	Rundll32 1	LSASS Memory	Virtualization/Sandbox Evasion 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)	Software Packing 2	Security Account Manager	Account Discovery 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)	Process Injection 1 1	NTDS	System Owner/User Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	System Information Discovery 1 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

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
86fa0c16_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
86fa0c16_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.4e30000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

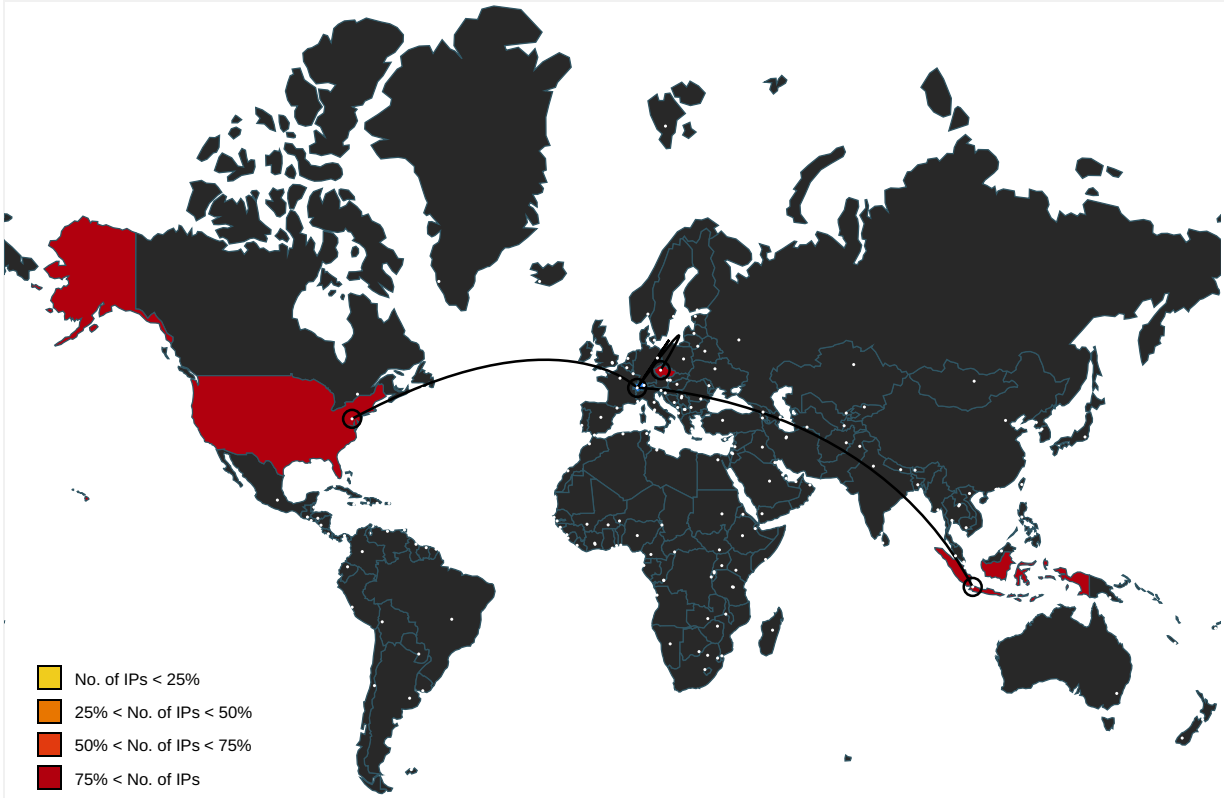
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413052
Start date:	13.05.2021
Start time:	07:06:01

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	86fa0c16_by_Libranalysis (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.winDLL@6/4@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 60.7% (good quality ratio 51%) • Quality average: 63.2% • Quality standard deviation: 37.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Simulations

Behavior and APIs

Time	Type	Description
07:07:32	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
UNIFIEDLAYER-AS-1US	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.209.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f61ac75de56cc9eee01d59a3e035a3dcadd9f_82810a17_1af78400\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12484
Entropy (8bit):	3.7680934848682273
Encrypted:	false
SSDEEP:	192:+aOim0oXDPSHBUZMX4jed+uG/u7spS274ItWcD:SiAXuBUZMX4jeK/u7spX4ItWcD
MD5:	41644315B7A75A619591E65D9AE54958
SHA1:	EC19DDA3204D836F341609C5B6DD44EC242CD9D2
SHA-256:	66C8C70BB98AE2700C1D4F76F8E90E7626C7004860466FF9FDF11646D5C5E2FF
SHA-512:	D7AD09D75B62598EDF715A6294D2CCAFAADD94DD117970BCFA3E6D27635E0BD3264C70227F5C81D2C032A88CB955A059B69B2B7605AB2BD9B209D919B06FE88
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.5.3.8.8.4.4.5.3.9.3.5.2.0.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.6.5.3.8.8.4.5.0.8.9.3.5.1.5.2.....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.=.4.e.1.5.7.6.0.0.-.3.d.5.3.-.4.7.a.9.-.9.8.3.6.-.5.e.3.d.4.9.f.8.e.f.3.5.....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.=.5.a.0.b.4.d.2.7.-.2.b.7.6.-.4.5.4.f.-.8.b.e.3.-.3.e.f.0.6.4.2.9.c.0.6.5.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.b.9.4.-.0.0.0.1.-.0.0.1.6.-.5.7.d.7.-.f.2.3.9.0.1.4.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:07:26 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	52702
Entropy (8bit):	2.038777510796249
Encrypted:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	
SSDEEP:	192:cc6wiNvb1V0sIfGRS5Ts44JDpKpiqKz+PGQXVJElOOwnNnKa:p1iNvb16u05Ts4upWi2GiMlOVNKa
MD5:	E6E3A908CF394D1ACB34A5D8013547A5
SHA1:	F32FF3E0A7888D07A90D914E0380297D192D1EFE
SHA-256:	D07BB01FF12AB4AA040C89C8DFECA5828CB4A8FD708BE5BF9DB7A5E959B16BCE
SHA-512:	991572F4102BF04CE2FF26461CCB067D3F50BAFA9E53C18A3A5C5569518D2241D05898CA9F858652FE500CF507B9D89FAF1A3396707E885FB377CBCF3C53D587
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....2.`.....U.....B.....GenuineIntelW.....T.....}2.`.....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\WER6EB3.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):	3.6964260079430744
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNicq6Vg6YHA6iygmfTXLShqCprj89bGknpsf2Qym:RrlsNi56i6Yg6iygmfTbSwGknCftj
MD5:	6AB06138258AB00AC739367738CF5AF6
SHA1:	427E5C4CA6F2A4636A3E4BE47EA856734E0992DF
SHA-256:	1D60C4BAE8AD83CF0A88FADECA308CE5F7552F6CDB463EAFA1195CB28D93D4EA
SHA-512:	D5285CA810FCD88D0804793519C4F76507EB027D4F81708A62ABAF259AC9DCA6C8D844C06D33AF09E1E65C3AB372532DEF8DF7B94CE5C5F80971C38C62C04FD
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.>.2.9.6.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER70E7.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):	4.475180841238783
Encrypted:	false
SSDEEP:	48:cvIwSD8zs8JgtWI9g+WSC8Bk8fm8M4JCdslNpFd+q8/cNFE4SrSjd:uITf6X/SN3JPNxfNqDWjd
MD5:	386BEE419325F222DE7A08E97CE73453
SHA1:	6B567D4830B730B7179ABED1CD7AF384776D9804
SHA-256:	1CB2C2847012991474515AB7947E7A493D9BA09A824B1BD7AFCAC001E15DAF49
SHA-512:	E6DA2B48A9FC918BECB653C659554C300DB91522E2DA61CD379E46A9D7967B6EE5502E1E9740AD09811AC8D5ED60B575F99ADC209FB0337845E3CFA96B0CE4E
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="987798" />.. <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):	7.51032805952502

General

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:	86fa0c16_by_Libranalysis.dll
File size:	167424
MD5:	86fa0c1657be46ef9d0e80b7cf46f930
SHA1:	d5a06060a0b0527c307e4db474bb1438c6507d63
SHA256:	e766f64fbc9a86d1561cf6517b5cab9c2cbd00a2e4d31e9a03ec69c09cdb942a
SHA512:	dcd6cac36853e892bdb4c5c6a086a0da12914b7e86a427f359a19456c25a7456d2751667dfe354034c750adbf982322df6fa606e3e0ff3258072ea7d239c2c99
SSDEEP:	3072:2ar6Ys6p54kfdo+APr0aYSbeO6aal8jeytFQTOpp2J:ws4p+ADxnSO6D2cOp
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:	0x10024b60
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:	0x609C7F99 [Thu May 13 01:23:37 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:	a5d8d3bddce161fe65c4f476bd18c6da

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

Instruction
mov eax, esi
mov dword ptr [10029728h], eax
jne 00007F87B4941836h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2770a	0x5b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x277d8	0x59	.rdata
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	0x23c9e	0x23e00	False	0.753620426829	data	7.52981613282	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2d41	0x2c00	False	0.749112215909	data	7.3747682631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.crt	0x28000	0x333c	0x1800	False	0.8125	MMDF mailbox	7.51564718747	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	0x268	0x400	False	0.5439453125	data	4.2612921869	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
CLUSAPI.dll	ClusterEnum
USER32.dll	TranslateMessage
KERNEL32.dll	LoadLibraryW, GetProfileSectionW, GetProfileSectionA, OpenSemaphoreW, CreateFileW, OutputDebugStringA, CloseHandle
ole32.dll	CreatePointerMoniker, CreateStreamOnHGlobal
ADVAPI32.dll	RegOverridePredefKey
RASAPI32.dll	RasGetConnectionStatistics

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

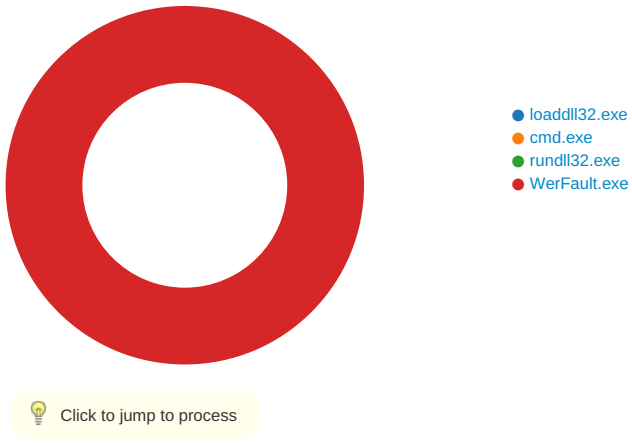
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:06:45.103411913 CEST	53784	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:45.113120079 CEST	65307	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:45.157262087 CEST	64344	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:45.160410881 CEST	53	53784	8.8.8.8	192.168.2.5
May 13, 2021 07:06:45.161808968 CEST	53	65307	8.8.8.8	192.168.2.5
May 13, 2021 07:06:45.228193998 CEST	53	64344	8.8.8.8	192.168.2.5
May 13, 2021 07:06:45.279907942 CEST	62060	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:45.331144094 CEST	53	62060	8.8.8.8	192.168.2.5
May 13, 2021 07:06:45.478935957 CEST	61805	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:45.559622049 CEST	53	61805	8.8.8.8	192.168.2.5
May 13, 2021 07:06:45.998661995 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:46.047414064 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 07:06:46.858326912 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:46.907011032 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 07:06:47.643942118 CEST	61733	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:47.692661047 CEST	53	61733	8.8.8.8	192.168.2.5
May 13, 2021 07:06:48.134984970 CEST	65447	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:06:48.195302010 CEST	53	65447	8.8.8.8	192.168.2.5
May 13, 2021 07:06:48.404737949 CEST	52441	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:48.458547115 CEST	53	52441	8.8.8.8	192.168.2.5
May 13, 2021 07:06:49.646414995 CEST	62176	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:49.695266008 CEST	53	62176	8.8.8.8	192.168.2.5
May 13, 2021 07:06:50.812019110 CEST	59596	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:50.860812902 CEST	53	59596	8.8.8.8	192.168.2.5
May 13, 2021 07:06:51.867297888 CEST	65296	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:51.918982983 CEST	53	65296	8.8.8.8	192.168.2.5
May 13, 2021 07:06:52.821266890 CEST	63183	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:52.880978107 CEST	53	63183	8.8.8.8	192.168.2.5
May 13, 2021 07:06:53.807734966 CEST	60151	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:53.859954119 CEST	53	60151	8.8.8.8	192.168.2.5
May 13, 2021 07:06:57.352184057 CEST	56969	53	192.168.2.5	8.8.8.8
May 13, 2021 07:06:57.403553963 CEST	53	56969	8.8.8.8	192.168.2.5
May 13, 2021 07:07:11.246360064 CEST	55161	53	192.168.2.5	8.8.8.8
May 13, 2021 07:07:11.310507059 CEST	53	55161	8.8.8.8	192.168.2.5
May 13, 2021 07:07:30.213720083 CEST	54757	53	192.168.2.5	8.8.8.8
May 13, 2021 07:07:30.270891905 CEST	53	54757	8.8.8.8	192.168.2.5
May 13, 2021 07:07:31.709702969 CEST	49992	53	192.168.2.5	8.8.8.8
May 13, 2021 07:07:31.769661903 CEST	53	49992	8.8.8.8	192.168.2.5
May 13, 2021 07:07:46.729007006 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 07:07:46.792149067 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 07:08:24.465197086 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 07:08:24.524297953 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 07:08:31.587100029 CEST	64345	53	192.168.2.5	8.8.8.8
May 13, 2021 07:08:31.647177935 CEST	53	64345	8.8.8.8	192.168.2.5
May 13, 2021 07:08:46.042759895 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 07:08:46.100116968 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 07:08:58.672198057 CEST	54791	53	192.168.2.5	8.8.8.8
May 13, 2021 07:08:58.730926991 CEST	53	54791	8.8.8.8	192.168.2.5
May 13, 2021 07:08:59.820404053 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 07:08:59.880425930 CEST	53	50463	8.8.8.8	192.168.2.5
May 13, 2021 07:09:00.487185001 CEST	50394	53	192.168.2.5	8.8.8.8
May 13, 2021 07:09:00.553889036 CEST	53	50394	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 2316 Parent PID: 5632

General

Start time:	07:06:52
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\86fa0c16_by_Libranalysis.dll'
Imagebase:	0xa50000
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: 1544 Parent PID: 2316

General

Start time:	07:06:53
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\86fa0c16_by_Libranalysis.dll',#1
Imagebase:	0x150000
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: 2964 Parent PID: 1544

General

Start time:	07:06:53
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\86fa0c16_by_Libranalysis.dll',#1
Imagebase:	0x10a0000

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: 00000002.00000002.317136592.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6800 Parent PID: 2964

General

Start time:	07:07:23
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2964 -s 764
Imagebase:	0x380000
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	6D9C1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70E7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70E7.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f61ac75de56cc9eee01d59a3e035a3dcadd9f_82810a17_1af78400	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f61ac75de56cc9eee01d59a3e035a3dcadd9f_82810a17_1af78400\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D9B497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70E7.tmp	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	success or wait	1	6D9B4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	success or wait	1	6D9B4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70E7.tmp.xml	success or wait	1	6D9B4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7104.tmp.csv	success or wait	1	6D9B4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7461.tmp.txt	success or wait	1	6D9B4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 9e 32 9d 60 a4 05 12 00 00 00 00 00	MDMP..... .....2.`.....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	unknown	6	00 00 00 00 00 00	.....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.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 94 0b 00 00 7d 32 9d 60 08 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 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	.....U.....B..... ..GenuineIntelW.....T... .....}2.`..... .....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	6D9B497A	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp</td><td>unknown</td><td>716</td><td>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 aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
aa aa aa aa aa aa aa
2b 00 00 00 53 00 00
00 2b 00 00 00 2b 00
00 00 cf ee 00 10 02
69 10 03 00 00 00 00
00 00 00 00 cf ee 00
10 04 8b 0c b2 2c fe
02 01 9b ea 00 10 23
00 00 00 82 02 01 00
7c fd 02 01 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</td><td>............................
....
....
....
....................+...S...+.
..+........i..................
,.......#.......|...+.........
....
..............</td><td>success or wait</td><td>1</td><td>6D9B497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp</td><td>unknown</td><td>168</td><td>f0 15 00 00 00 00 00
00 05 00 00 c0 00 00
00 00 00 00 00 00 00
00 00 00 9b ea 00 10
00 00 00 00 02 00 00
00 00 00 00 00 01 00
00 00 00 00 00 00 04
8b 0c b2 ff ff ff ff 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 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</td><td>............................
....
....
....
....
..............%..</td><td>success or wait</td><td>1</td><td>6D9B497A</td><td>unknown</td></tr>
<tr><td>C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp</td><td>unknown</td><td>20</td><td>12 00 00 00 7c ed 02
01 00 00 00 00 84 12
00 00 cc 34 00 00</td><td>....|............4..</td><td>success or wait</td><td>18</td><td>6D9B497A</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	unknown	4740	bc 9a a2 77 a3 1a 32 77 aa aa aa aa b0 ef 02 01 aa aa aa aa 00 00 00 00 00 00 00 00 aa aa aa aa 00 00 00 00 f8 02 00 00 f4 02 00 00 00 00 00 00 24 00 00 00 aa aa aa aa 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 aa aa aa aa 00 70 3e 03 00 00 00 00 00 00 00 00 00 00 00 00 b0 ef 02 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...w..2w..................... ....$........... ....p >............................	success or wait	17	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	unknown	4096	f4 f9 e2 04 00 00 e3 04 00 40 e2 04 00 00 00 00 00 1e 00 00 00 00 00 00 00 30 3f 03 00 00 00 00 94 0b 00 00 a4 15 00 00 00 00 00 00 00 00 00 00 00 70 3e 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 9b 77 09 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.........@...............0?... ....p>......... ....p.w.............	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	unknown	4	04 00 00 00	....	success or wait	4	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.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 00 00 00 00 cf ee 00 10 00 00 00 00 10 ef 02 01 bc 9a a2 77 23 00 00 00 12 02 00 00 80 ed 02 01 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...+. ..+........................... ....w#...........+.........	success or wait	4	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	unknown	48	a4 15 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 30 3f 03 00 00 00 00 48 f8 e2 04 00 00 00 00 b8 07 00 00 44 52 00 00 cc 02 00 00 dc 30 00 00	....0?.....H..... ......DR.......0..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	unknown	4	33 00 00 00	3...	success or wait	51	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.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	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	unknown	752	00 00 05 74 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 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 04 00 00 00 00 b0 10 02 00 00 00 00 00 00 b9 02 00 00 00 00 3e 47 01 00 00 01 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 3a dc 00 00 00 00 00 00 46 48 03 00 00 00 00 00 b5 8e 02 00 00 00 00 00 ff ff ff ff 00 00 00 00 95 d3 21 00 00 00 00 00 40 ff 1f 00 00 00 00 00 34 eb 21 00 00 00 00	...t.....0...U..s@...%..... .....B.....B?..... .....#..... ..@A.....Zb..... .... >G.....:.....FH .....I..... @.....4.!....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	....E.v.e.n.t..... .....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(...W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t. .....I.R.T.i.m	success or wait	1	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER684A.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 24 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 c6 af 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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 39 00 36 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.9.6.4.<./.P.i.d.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0.0.0.<./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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 36 00 33 00 33 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.>.3.3.6.3.3.<./.U.p.t.i.m.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.8.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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 38 00 37 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.>.9.2.4.8.7.6.8.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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 38 00 37 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.4.8.7.6.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.6.4.0.<./.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.1.5.4.4.<./.P.i.d.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.0. <./.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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 39 00 34 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.3.9.4.1. <./.U.p.t.i.m.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.9.<./.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 33 00 35 00 35 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.3.5.5.5.2.<./.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 36 00 39 00 38 00 36 00 38 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.6.9.8.6.8.8.<./.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 39 00 32 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.5.9.2.9.6.<./.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 36 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.1.6.7.6.8.<./.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 39 00 32 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.5.9.2.9.6.<./.P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<./.P.a.r.e.n.t.P.r.o.c.e.s.s.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	8	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	6	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 61 00 75 00 6c 00 77 00 62 00 64 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.a.u.l.w.b.d.,. .I.n.c...<./.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 61 00 75 00 6c 00 77 00 62 00 64 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.a.u.l.w.b.d.7.,.1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 38 00 38 00 38 00 34 00 35 00 38 00 31 00 39 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e.>.1.5.8.8.8.4.5.8.1.9.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	3	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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 30 00 37 00 3a 00 32 00 37 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.:.0.7.:.2.7.Z.".>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 39 00 36 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 38 00 36 00 35 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 38 00 36 00 35 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.=.".3.3.8.". .P.I.D.=.".2.9.6.4.". .U.p.t.i.m.e.M.S.=.".2.8.6.5.6.". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.=.".2.8.6.5.6.". .S.u.s.p.e.n.d.e.d.M.S.=.".0.". .H.a.n.g.C.o.u.n.t.=.".0.". .G.h.o.s.t.C.o.u.n.t.=.".0.". .C.r.a.s.h.e.d	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 34 00 65 00 31 00 35 00 37 00 36 00 30 00 30 00 2d 00 33 00 64 00 35 00 33 00 2d 00 34 00 37 00 61 00 39 00 2d 00 39 00 38 00 33 00 36 00 2d 00 35 00 65 00 33 00 64 00 34 00 39 00 66 00 38 00 65 00 66 00 33 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.4.e.1.5.7.6.0.0.-.3.d.5.3.-.4.7.a.9.-.9.8.3.6.-.5.e.3.d.4.9.f.8.e.f.3.5.<./.G.u.i.d.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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 30 00 37 00 3a 00 32 00 37 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.:.0.7.:.2.7.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00	....	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6EB3.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	6D9B497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER70E7.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	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f61ac75de56cc9eee01d59a3e035a3dcadd9f_82810a17_1af78400\Report.wer	unknown	2	ff fe	..	success or wait	1	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f61ac75de56cc9eee01d59a3e035a3dcadd9f_82810a17_1af78400\Report.wer	unknown	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	V.e.r.s.i.o.n.=.1.....	success or wait	182	6D9B497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_f61ac75de56cc9eee01d59a3e035a3dcadd9f_82810a17_1af78400\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 35 00 35 00 37 00 38 00 31 00 31 00 39 00 36 00	M.e.t.a.d.a.t.a.H.a.s.h.=.-.1.5.5.7.8.1.1.9.6.	success or wait	1	6D9B497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	success or wait	1	6D9D36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D9D1FB2	RegCreateKeyExW
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9B43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D9D36BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LowerCaseLongPath	unicode	c:\windows\syswow64\rundll32.exe	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LongPathHash	unicode	rundll32.exe|ab97b57a	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Name	unicode	rundll32.exe	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Publisher	unicode	microsoft corporation	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinFileVersion	unicode	10.0.17134.1	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinaryType	unicode	pe32_i386	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	ProductVersion	unicode	10.0.17134.1	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	LinkDate	unicode	01/30/1986 11:42:44	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	BinProductVersion	unicode	10.0.17134.1	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Size	B	00 F2 00 00 00 00 00 00	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	Language	dword	1033	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsPeFile	dword	1	success or wait	1	6D9D36BF	unknown
\REGISTRY\A\{5d1cfc62-e678-d45d-78ee-5a9122ff4a10}\Root\InventoryApplicationFile\rundll32.exe|ab97b57a	IsOsComponent	dword	1	success or wait	1	6D9D36BF	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 9B EA 00 10 02 00 00 00 01 00 00 00 04 8B 0C B2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6D9D1FE8	RegSetValueExW

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

Disassembly

Code Analysis