

JOeSandbox Cloud BASIC



ID: 413048

Sample Name:

27c06d28_by_Libranalysis

Cookbook: default.jbs

Time: 06:58:13

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 27c06d28_by_Libranalysis	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Dridex	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Networking:	5
E-Banking Fraud:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	8
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	10
ASN	10
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	13
General	13
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Rich Headers	14
Data Directories	14
Sections	15
Resources	15
Imports	15
Version Infos	15
Network Behavior	15

UDP Packets	15
Code Manipulations	17
Statistics	17
Behavior	17
System Behavior	17
Analysis Process: loadll32.exe PID: 7036 Parent PID: 5880	17
General	17
File Activities	18
Analysis Process: cmd.exe PID: 7044 Parent PID: 7036	18
General	18
File Activities	18
Analysis Process: rundll32.exe PID: 7056 Parent PID: 7044	18
General	18
Analysis Process: WerFault.exe PID: 6888 Parent PID: 7056	18
General	18
File Activities	19
File Created	19
File Deleted	19
File Written	19
Registry Activities	41
Key Created	41
Key Value Created	41
Disassembly	42
Code Analysis	42

Analysis Report 27c06d28_by_Libranalysis

Overview

General Information

Sample Name:	27c06d28_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	413048
MD5:	27c06d28a76580..
SHA1:	147d9851ebc37e..
SHA256:	41ee518bd4c9dfa.
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Dridex

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

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected Dridex unpacked file

C2 URLs / IPs found in malware con...

Machine Learning detection for samp...

Checks if the current process is bein...

Contains functionality to check if a d...

Contains functionality to query locale...

Creates a DirectInput object (often fo...

Creates a process in suspended mo...

Detected potential crypto function

IP address seen in connection with o...

Internet Provider seen in connection...

Classification

Startup

System is w10x64

loadll32.exe (PID: 7036 cmdline: loadll32.exe 'C:\Users\user\Desktop\27c06d28_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 7044 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\27c06d28_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 7056 cmdline: rundll32.exe 'C:\Users\user\Desktop\27c06d28_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 6888 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7056 -s 764 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)

cleanup

Malware Configuration

Threatname: Dridex

```
{
  "Version": 22201,
  "C2 list": [
    "43.229.206.212:443",
    "82.209.17.209:8172",
    "162.241.209.225:4125"
  ],
  "RC4 keys": [
    "16dkGSt0zdHgjuCciXGdSX7UrHmfYSUG8wEUtKNgzHrWMfTGafJbC",
    "39t3NdDhurvpLtfNCpva5goSylkxjIBtIwMPTv1DPbNEcuIekQC70"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
--------	------	-------------	--------	---------

Copyright Joe Security LLC 2021

Page 4 of 42

Source	Rule	Description	Author	Strings
00000002.00000002.741171376.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

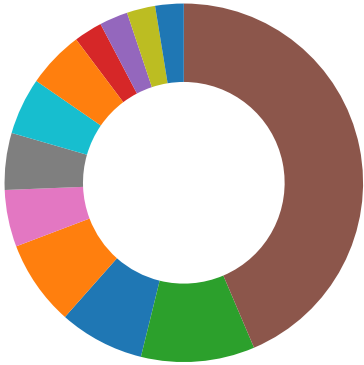
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:

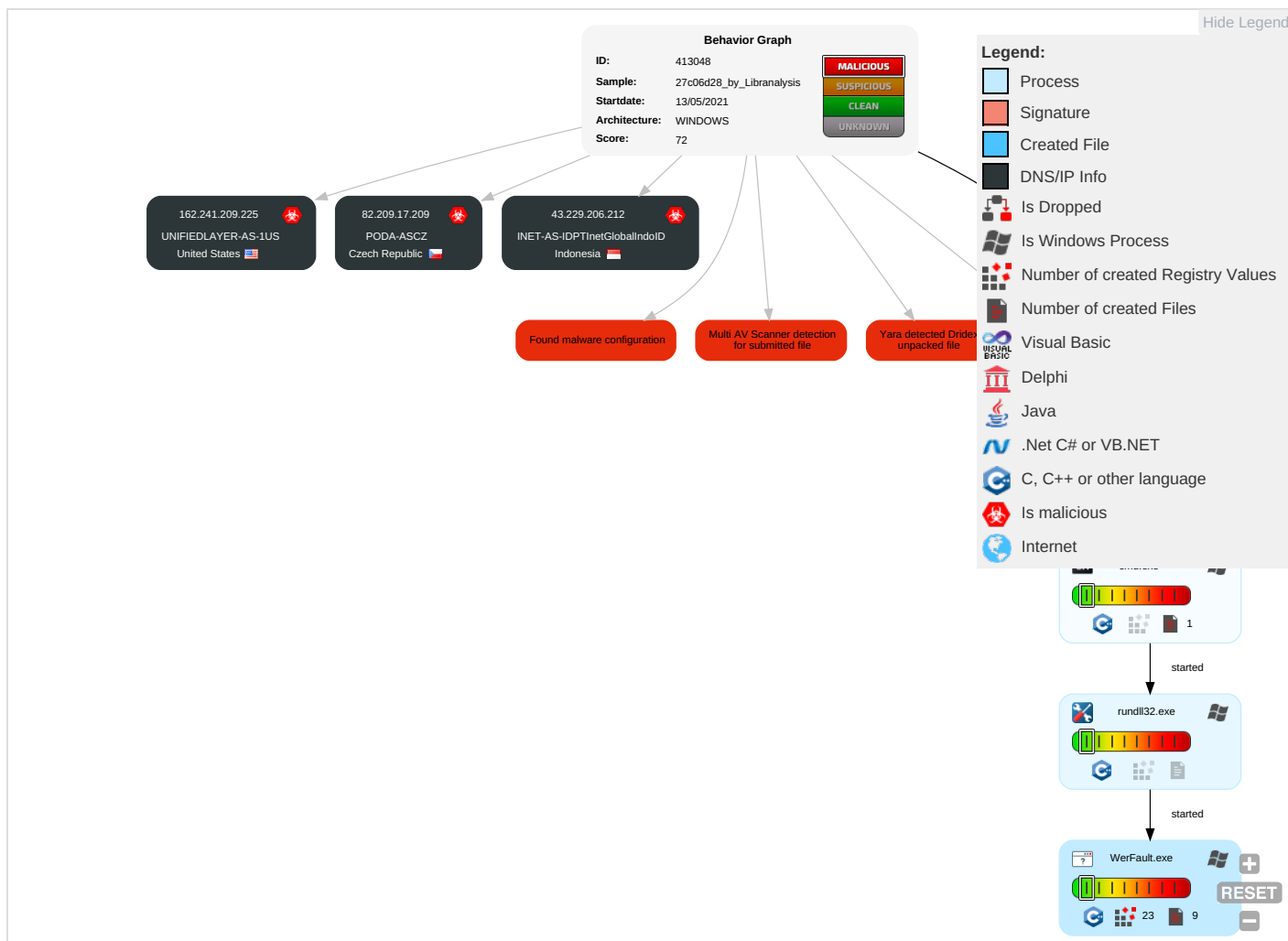


Yara detected Dridex unpacked file

Mitre Att&ck Matrix

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

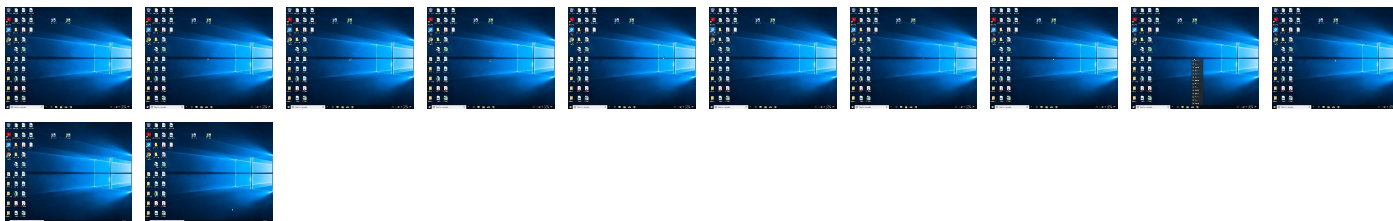
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
27c06d28_by_Libranalysis.dll	30%	ReversingLabs	Win32.Trojan.Convagent	
27c06d28_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.4b30000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

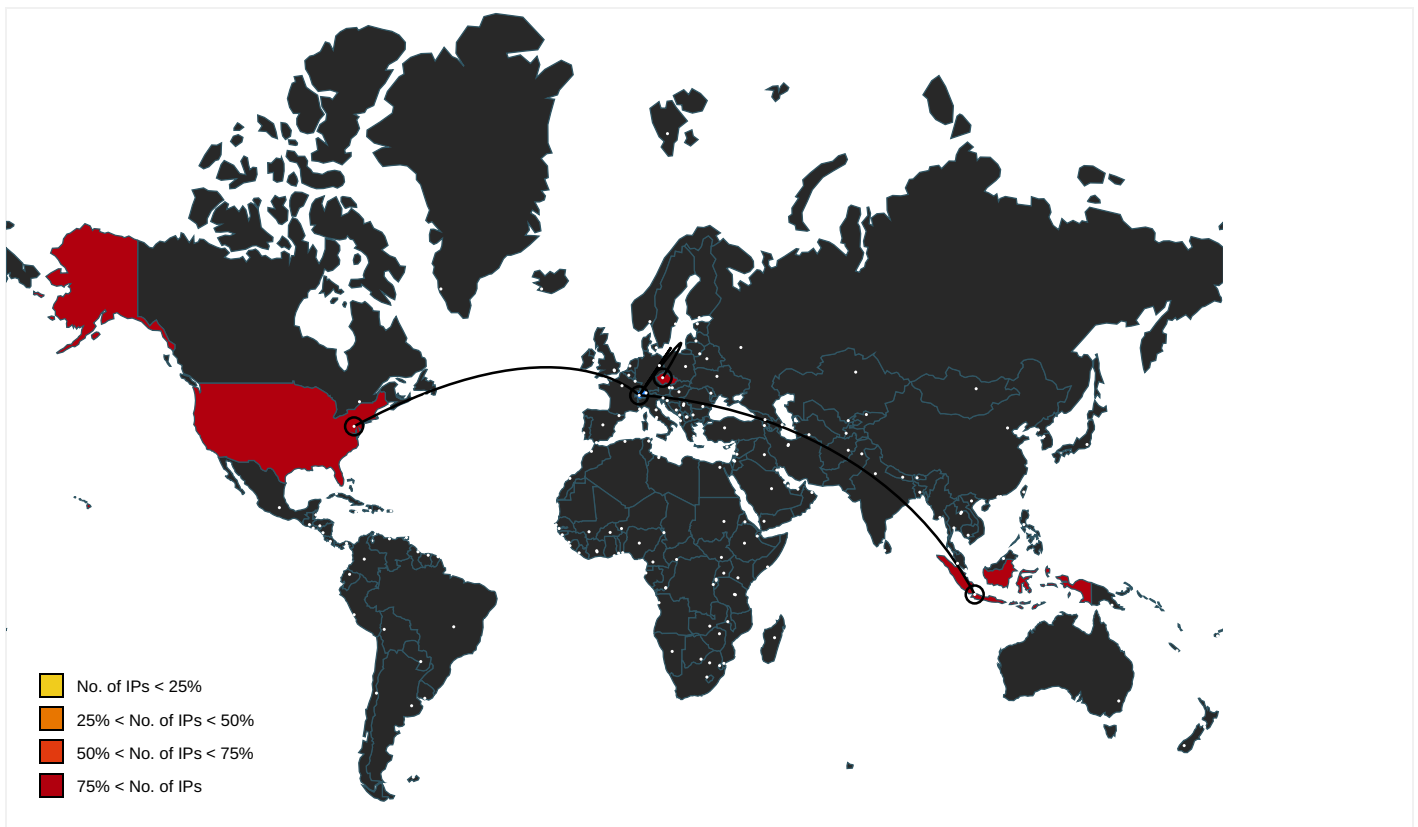
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/09/policyu2u	WerFault.exe, 0000000C.00000000 2.737695519.00000000004C3D000.0 0000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policy	WerFault.exe, 0000000C.00000000 2.737695519.00000000004C3D000.0 0000004.00000001.sdmp	false		high

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

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
43.229.206.212	unknown	Indonesia		24532	INET-AS-IDPTInetGlobalIndoID	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413048
Start date:	13.05.2021
Start time:	06:58:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	27c06d28_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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 57.1% (good quality ratio 49.2%) • Quality average: 67.3% • Quality standard deviation: 35.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Simulations

Behavior and APIs

Time	Type	Description
06:59:42	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	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	
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	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
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
UNIFIEDLAYER-AS-1US	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	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
	a13bac07_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	0f6f2d53_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
	634459e1_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	0ee1d71e_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_816d2b9bf3dcde33e3529c74b8a21b9d25159d_82810a17_1a8a03bclReport.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12480
Entropy (8bit):	3.766600518355167
Encrypted:	false
SSDEEP:	192:GSlii0xOdcHBUZMX4jed+RG/u7suS274ltWc1b:vikXgBUZMX4je9/u7suX4ltWc1b
MD5:	BD4AB325E8E68D2CFA1AD9CD0A8FE656
SHA1:	A37BB023434D529D38622AEC65FF6B1078F9F373
SHA-256:	7D2F1FDD6514789DD89E0F8500078E490C996B560D3CF399FA41E7698D2A54CC
SHA-512:	882F8C8AA9F8ADF828EE78A7E51C4B72D5D37414A37785D528EF91E35279518C23DAE28870AF0E189D018656AEEA34B12D29CBB30DDBABA208CBC738900C351

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_816d2b9bf3dcde33e3529c74b8a21b9d25159d_82810a17_1a8a03bclReport.wer	
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=1.3.2.6.5.3.5.5.5.7.3.8.8.3.7.0.8.9.....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.=1.3.2.6.5.3.5.5.8.0.8.2.1.1.8.4.1.....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.=e.f.2.d.2.d.c.b.-e.a.9.5.-4.f.a.4.-b.2.c.0.-8.d.8.3.0.3.e.9.8.5.1.2.....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.=7.3.a.2.0.4.d.5.-f.9.c.4.-4.5.c.e.-8.1.a.4.-d.d.8.6.8.c.c.9.4.e.1.9.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.1.b.9.0.-0.0.0.1.-0.0.1.b.-a.7.7.e.-2.6.b.0.b.4.4.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=W...0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE094.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 04:59:36 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	39390
Entropy (8bit):	2.3437944998552465
Encrypted:	false
SSDEEP:	192:DNpc/8jZ9t+jHsUTOTj19Hblln0AqXr6sXTahkqm:RsDNK19IAq2sXeKN
MD5:	63A24B3D8BE8BDB35B6D8D42B3F7CEBE
SHA1:	E1B166D6767FC45706A226ABDC1269FFBB2B9A1D
SHA-256:	AEA804F42987A94B2817F37ACDCB0FED9453375065DC874D118D37E201098250
SHA-512:	532C21B17BC7DEF48C3C447E384668C0F749B1C81CDB78889EF30A3248301E46D849447B096C01D20ECE3BE6B2030F14C00B98768F16E8390D7F1027D6AE2ED
Malicious:	false
Reputation:	low
Preview:	MDMP.....8..`.....U.....B.....x.....GenuineIntelW.....T.....`.....0.=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERE95F.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):	8294
Entropy (8bit):	3.6933933242307155
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi5c6kR6YU069gKGgmfTkVS0+prC89bBdsfWwrm:RrlsNii6C6Y/69EgmftTsSTBWfe
MD5:	261E7B1AB43061D24FDB3EF26272B0A6
SHA1:	017E6C8445669A72D76106A6FEFC78F5D7A82E2E
SHA-256:	885F44070BA87EB79E2D0326C5D6A2D20FC031A0E9AC0B98A5368EFD1A609D1
SHA-512:	0FA1DC20DB71CAD5FFC1851BDBD4FA78A7986AA246336B396BB004279F9219564508243FB3B72C251487A674D73701237E846E5A16BEE97FE4AA6347D64DE53F
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.-16."?>.....<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>7.0.5.6.</P.i.d>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBE1.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):	4.472910307037702
Encrypted:	false
SSDEEP:	48:cvlwSD8zsnJgtWI92xyWSC8BZXM8fm8M4JCds8NrFIQ+q8/pNFnkn4SrSmd:ulTfJhRSNrXxJ6NgqNwDWmd
MD5:	2C94E4B7A65AF0886B39E420AC1B6171
SHA1:	27FC5D6B2F6352C2F43B311E64C82A380C903DC9
SHA-256:	420B0D1F5E5345C9E9F1D3814DF1E113A9B9C1CA123519F35F2881AA6FEC6FF5
SHA-512:	21EE18B1B06BBA063FEA9DFDCDA9FEB66F90064948CF04ED2710168A6B9BDBF4254EBA580258E5EEAE4A3ED9906DDEE4AB92BD443CAABE15A2B1E4A206047CA9
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBE1.tmp.xml

Preview: <?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="987250" />.. <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):	7.513902607405205
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:	27c06d28_by_Libranalysis.dll
File size:	167424
MD5:	27c06d28a765800b39f02141c68c1aa5
SHA1:	147d9851ebc37e63b43cc1755d49b7810ae67db5
SHA256:	41ee518bd4c9dfa11d4c6226f67a34e1df45101b0e047ee68d1653eec84353c9
SHA512:	3dd15e09adb33904dc8c20f4308c2a45c3c38a4bd0822de086b248fd377749e92682b4edab45006ea80ef3c5827b72db3ca8a76a0afde776617f018a50c200b8
SSDEEP:	3072:z9F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj;z9F6rQXvFczyYpQP
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode....\$.Xm.o...<...<...U!<...<.B<r...<...<rQ!<...<...<...<3..<au.<...<sz!<...<Rich...<.....

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10024cc0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609C7F93 [Thu May 13 01:23:31 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	88962f6760ea005847fb88b87e8ce1fd

Entrypoint Preview

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x23dfe	0x23e00	False	0.756362968206	data	7.53078515147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x331c	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x3a0	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0xfd5	0x400	False	0.548828125	data	4.2946697642	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Version Infos

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:58:54.276034117 CEST	65298	53	192.168.2.4	8.8.8.8
May 13, 2021 06:58:54.287487030 CEST	59123	53	192.168.2.4	8.8.8.8
May 13, 2021 06:58:54.333271980 CEST	53	65298	8.8.8.8	192.168.2.4

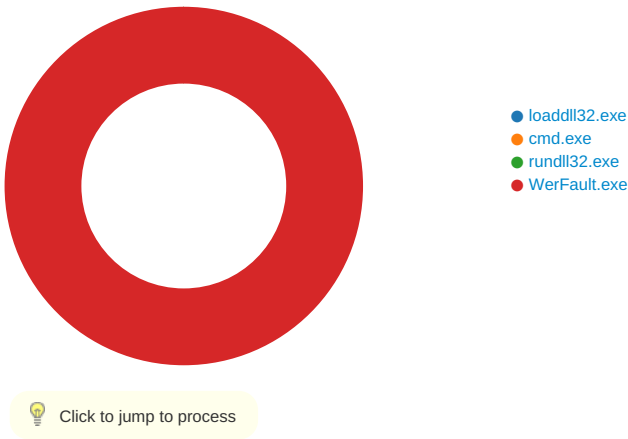
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:58:54.354753971 CEST	53	59123	8.8.8.8	192.168.2.4
May 13, 2021 06:58:55.079174042 CEST	54531	53	192.168.2.4	8.8.8.8
May 13, 2021 06:58:55.136126041 CEST	53	54531	8.8.8.8	192.168.2.4
May 13, 2021 06:58:55.966430902 CEST	49714	53	192.168.2.4	8.8.8.8
May 13, 2021 06:58:56.018066883 CEST	53	49714	8.8.8.8	192.168.2.4
May 13, 2021 06:58:56.903609991 CEST	58028	53	192.168.2.4	8.8.8.8
May 13, 2021 06:58:56.962311983 CEST	53	58028	8.8.8.8	192.168.2.4
May 13, 2021 06:58:58.783267975 CEST	53097	53	192.168.2.4	8.8.8.8
May 13, 2021 06:58:58.832999945 CEST	53	53097	8.8.8.8	192.168.2.4
May 13, 2021 06:59:01.687031984 CEST	49257	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:01.735799074 CEST	53	49257	8.8.8.8	192.168.2.4
May 13, 2021 06:59:03.347151041 CEST	62389	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:03.400690079 CEST	53	62389	8.8.8.8	192.168.2.4
May 13, 2021 06:59:04.303529978 CEST	49910	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:04.357237101 CEST	53	49910	8.8.8.8	192.168.2.4
May 13, 2021 06:59:05.941963911 CEST	55854	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:05.995593071 CEST	53	55854	8.8.8.8	192.168.2.4
May 13, 2021 06:59:08.392894030 CEST	64549	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:08.447360992 CEST	53	64549	8.8.8.8	192.168.2.4
May 13, 2021 06:59:09.643337965 CEST	63153	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:09.692065001 CEST	53	63153	8.8.8.8	192.168.2.4
May 13, 2021 06:59:10.884350061 CEST	52991	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:10.935985088 CEST	53	52991	8.8.8.8	192.168.2.4
May 13, 2021 06:59:11.980807066 CEST	53700	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:12.029700041 CEST	53	53700	8.8.8.8	192.168.2.4
May 13, 2021 06:59:13.317476988 CEST	51726	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:13.366441011 CEST	53	51726	8.8.8.8	192.168.2.4
May 13, 2021 06:59:14.097076893 CEST	56794	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:14.145761967 CEST	53	56794	8.8.8.8	192.168.2.4
May 13, 2021 06:59:18.756556988 CEST	56534	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:18.808933973 CEST	53	56534	8.8.8.8	192.168.2.4
May 13, 2021 06:59:19.892052889 CEST	56627	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:19.942194939 CEST	53	56627	8.8.8.8	192.168.2.4
May 13, 2021 06:59:20.716880083 CEST	56621	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:20.765548944 CEST	53	56621	8.8.8.8	192.168.2.4
May 13, 2021 06:59:21.677486897 CEST	63116	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:21.729594946 CEST	53	63116	8.8.8.8	192.168.2.4
May 13, 2021 06:59:22.648226023 CEST	64078	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:22.697113037 CEST	53	64078	8.8.8.8	192.168.2.4
May 13, 2021 06:59:30.084342003 CEST	64801	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:30.141482115 CEST	53	64801	8.8.8.8	192.168.2.4
May 13, 2021 06:59:37.194602013 CEST	61721	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:37.253611088 CEST	53	61721	8.8.8.8	192.168.2.4
May 13, 2021 06:59:42.187860012 CEST	51255	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:42.236614943 CEST	53	51255	8.8.8.8	192.168.2.4
May 13, 2021 06:59:48.839135885 CEST	61522	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:48.899328947 CEST	53	61522	8.8.8.8	192.168.2.4
May 13, 2021 06:59:54.034141064 CEST	52337	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:54.086162090 CEST	53	52337	8.8.8.8	192.168.2.4
May 13, 2021 06:59:54.613600969 CEST	55046	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:54.673302889 CEST	53	55046	8.8.8.8	192.168.2.4
May 13, 2021 06:59:55.309428930 CEST	49612	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:55.371252060 CEST	53	49612	8.8.8.8	192.168.2.4
May 13, 2021 06:59:55.873225927 CEST	49285	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:55.930465937 CEST	53	49285	8.8.8.8	192.168.2.4
May 13, 2021 06:59:55.970274925 CEST	50601	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:56.028713942 CEST	53	50601	8.8.8.8	192.168.2.4
May 13, 2021 06:59:56.602158070 CEST	60875	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:56.651154995 CEST	53	60875	8.8.8.8	192.168.2.4
May 13, 2021 06:59:57.348642111 CEST	56448	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:57.408096075 CEST	53	56448	8.8.8.8	192.168.2.4
May 13, 2021 06:59:57.889067888 CEST	59172	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:57.946173906 CEST	53	59172	8.8.8.8	192.168.2.4
May 13, 2021 06:59:58.768136978 CEST	62420	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 06:59:58.825294971 CEST	53	62420	8.8.8.8	192.168.2.4
May 13, 2021 06:59:59.804605961 CEST	60579	53	192.168.2.4	8.8.8.8
May 13, 2021 06:59:59.853250027 CEST	53	60579	8.8.8.8	192.168.2.4
May 13, 2021 07:00:00.342619896 CEST	50183	53	192.168.2.4	8.8.8.8
May 13, 2021 07:00:00.393718958 CEST	53	50183	8.8.8.8	192.168.2.4
May 13, 2021 07:00:11.153641939 CEST	61531	53	192.168.2.4	8.8.8.8
May 13, 2021 07:00:11.212196112 CEST	53	61531	8.8.8.8	192.168.2.4
May 13, 2021 07:00:45.038569927 CEST	49228	53	192.168.2.4	8.8.8.8
May 13, 2021 07:00:45.096081018 CEST	53	49228	8.8.8.8	192.168.2.4
May 13, 2021 07:00:46.782470942 CEST	59794	53	192.168.2.4	8.8.8.8
May 13, 2021 07:00:46.841753006 CEST	53	59794	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 7036 Parent PID: 5880

General

Start time:	06:58:59
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\27c06d28_by_Libranalysis.dll'
Imagebase:	0xac0000
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: 7044 Parent PID: 7036

General

Start time:	06:59:00
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\27c06d28_by_Libranalysis.dll',#1
Imagebase:	0x11d0000
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: 7056 Parent PID: 7044

General

Start time:	06:59:00
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\27c06d28_by_Libranalysis.dll',#1
Imagebase:	0x3b0000
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: 00000002.00000002.741171376.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6888 Parent PID: 7056

General

Start time:	06:59:31
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7056 -s 764
Imagebase:	0x1210000
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	6F571717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE094.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE094.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBE1.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBE1.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_816d2b9bf3dcde33e3529c74b8a21b9d25159d_82810a17_1a8a03bc	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_816d2b9bf3dcde33e3529c74b8a21b9d25159d_82810a17_1a8a03bc\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6F56497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE094.tmp	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBE1.tmp	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE094.tmp.dmp	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBE1.tmp.xml	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBFE.tmp.csv	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFE7.tmp.txt	success or wait	1	6F564BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE094.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 38 b2 9c 60 a4 05 12 00 00 00 00 00	MDMP.....8..`.....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE094.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	6F56497A	unknown

[illegible]

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE094.tmp.dmp	unknown	108	03 00 00 00 64 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 6c 07 00 00 05 00 00 00 c4 00 00 00 b0 2d 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 c6 7b 00 00 15 00 00 00 ec 01 00 00 f4 1c 00 00 16 00 00 00 98 00 00 00 e0 1e 00 00	...d.....l.....-T.....8..... ...T.....`...{.....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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.-16."?>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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.l.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.0.5.6.</.P.i.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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.I.I.3.2...e.x.e.</.I.m.a.g.e.N.a.m.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 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.</.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 35 00 36 00 35 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.5.6.5.5.<./U.p.t.i.m.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	<.l.p.t.E.n.a.b.l.e.d.>.0.<./l.p.t.E.n.a.b.l.e.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 38 00 31 00 35 00 36 00 38 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.>.1.2.7.8.1.5.6.8.0.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 36 00 37 00 36 00 37 00 31 00 30 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.6.7.6.7.1.0.4.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 33 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.>.2.7.0.3.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 30 00 39 00 33 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.0.9.3.1.2.0.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 30 00 32 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 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.>.9.0.9.3.1.2.0.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.4.1.6.<./Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.2.8.9.8.4.<./Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 37 00 31 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 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.2.8.7.1.2.<./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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 36 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.i.e.U.s.a.g.e>.5.6.6.8.8.6.4.<./P.a.g.e.f.i.i.e.U.s.a.g.e>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 39 00 38 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.9.8.2.4.0.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 36 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.6.6.8.8.6.4.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.7.0.4.4.<./P.i.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	<.l.m.a.g.e.N.a.m.e.>.c.m.d...e.x.e.<./l.m.a.g.e.N.a.m.e.>.	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.0.0.0.0.0.0.0.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 35 00 39 00 39 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<U.p.t.i.m.e>.3.5.9.9.6.<./U.p.t.i.m.e>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	<.l.p.t.E.n.a.b.l.e.d>.0.<./l.p.t.E.n.a.b.l.e.d>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.0.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 32 00 37 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.2.7.3.6.0.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 34 00 38 00 31 00 36 00 30 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.4.8.1.6.0.0.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 31 00 31 00 30 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.5.1.1.0.4.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 30 00 34 00 34 00 38 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.>.3.6.0.4.4.8.0.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 31 00 31 00 30 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.5.1.1.0.4.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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.I.I.3.2...e.x.e.<./P.a.r.a.m.e.t.e.r.0>.	success or wait	8	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 77 00 75 00 61 00 63 00 67 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.>.w.u.a.c.g.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 77 00 75 00 61 00 63 00 67 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>.w.u.a.c.g.d.7.,.1.</.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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.</.B.I.O.S.V.e.r.s.i.o.n>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 36 00 36 00 39 00 33 00 37 00 38 00 36 00 32 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e>.1.5.6.6.9.3.7.8.6.2.</.O.S.I.n.s.t.a.l.l.D.a.t.e>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	70	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 2d 00 30 00 31 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.>-.0.1.:.0.0.<./T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 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.<./F.l.a.g.s.>.	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 30 00 34 00 3a 00 35 00 39 00 3a 00 33 00 36 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.0.4.:.5.9.: 3.6.Z.">.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 36 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 35 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 30 00 32 00 30 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 30 00 32 00 30 00 33 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 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.= ".3.6.4". .P.I.D.= ".7.0.5.6". .U.p.t.i.m.e.M.S.= ".3.0.2.0.3". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".3.0.2.0.3". .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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 65 00 66 00 32 00 64 00 32 00 64 00 63 00 62 00 2d 00 65 00 61 00 39 00 35 00 2d 00 34 00 66 00 61 00 34 00 2d 00 62 00 32 00 63 00 30 00 2d 00 38 00 64 00 38 00 33 00 30 00 33 00 65 00 39 00 38 00 35 00 31 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.e.f.2.d.2.d.c.b.-.e.a.9.5.-.4.f.a.4.-.b.2.c.0.-.8.d.8.3.0.3.e.9.8.5.1.2.<./G.u.i.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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 30 00 34 00 3a 00 35 00 39 00 3a 00 33 00 36 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.0.4.:5.9.:3.6.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE95F.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	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBE1.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"?>.. ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_816d2b9bf3dcde33e3529c74b8a21b9d25159d_82810a17_1a8a03bc\Report.wer	unknown	2	ff fe	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_816d2b9bf3dcde33e3529c74b8a21b9d25159d_82810a17_1a8a03bc\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	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_816d2b9bf3dcde33e3529c74b8a21b9d25159d_82810a17_1a8a03bc\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 38 00 37 00 34 00 39 00 36 00 37 00 33 00 35 00	M.e.t.a.d.a.t.a.H.a.s.h.=.- .6.8.7.4.9.6.7.3.5.	success or wait	1	6F56497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRYA\{a3b2d3b8-ba74-0ee0-71f4-eaf1724fb0c4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5836BF	unknown
\REGISTRYA\{a3b2d3b8-ba74-0ee0-71f4-eaf1724fb0c4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5836BF	unknown
\REGISTRYA\{a3b2d3b8-ba74-0ee0-71f4-eaf1724fb0c4}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6F5836BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F581FB2	RegCreateKeyExW
\REGISTRYA\{a3b2d3b8-ba74-0ee0-71f4-eaf1724fb0c4}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{a3b2d3b8-ba74-0ee0-71f4-eaf1724fb0c4}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6F5836BF	unknown
\REGISTRYA\{a3b2d3b8-ba74-0ee0-71f4-eaf1724fb0c4}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6F5836BF	unknown

