

JoeSandbox Cloud BASIC



ID: 413050

Sample Name:

13f88d67_by_Libranalysis.dll

Cookbook: default.jbs

Time: 07:09:38

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 13f88d67_by_Libranalysis.dll	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	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
Contacted IPs	8
Public	8
General Information	8
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	12
General	13
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Rich Headers	14
Data Directories	14
Sections	14
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: 6944 Parent PID: 6072	17
General	17
File Activities	17
Analysis Process: cmd.exe PID: 6960 Parent PID: 6944	17
General	17
File Activities	18
Analysis Process: rundll32.exe PID: 6976 Parent PID: 6960	18
General	18
Analysis Process: WerFault.exe PID: 6744 Parent PID: 6976	18
General	18
File Activities	18
File Created	18
File Deleted	19
File Written	19
Registry Activities	41
Key Created	41
Key Value Created	41
Disassembly	42
Code Analysis	42

Analysis Report 13f88d67_by_Libranalysis.dll

Overview

General Information

Sample Name:

13f88d67_by_Libranalysis.dll

Analysis ID:

413050

MD5:

13f88d6731bf769..

SHA1:

6f3536a9dde8f77..

SHA256:

3a6248e07dc73d..

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 process in suspended mo...

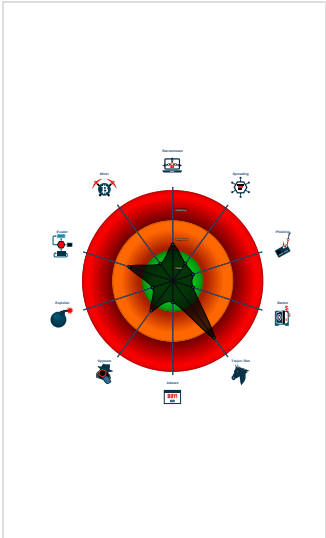
Detected potential crypto function

IP address seen in connection with o...

Internet Provider seen in connection...

Monitors certain registry keys / valu...

Classification



Startup

System is w10x64

loadll32.exe (PID: 6944 cmdline: loadll32.exe 'C:\Users\user\Desktop\13f88d67_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 6960 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\13f88d67_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 6976 cmdline: rundll32.exe 'C:\Users\user\Desktop\13f88d67_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 6744 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6976 -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": [

"16dkGStOzdHgjuCciXGdSX7UrHkfYSUG8wEUtKNgzHrWMfTGafJbc",

"39t3NdDhurvp1tFNCpvA5goSylkxjIBtIwHPTv1DPbNEcuIekQC70"

]

}

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.760132699.0000000010001000.0000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

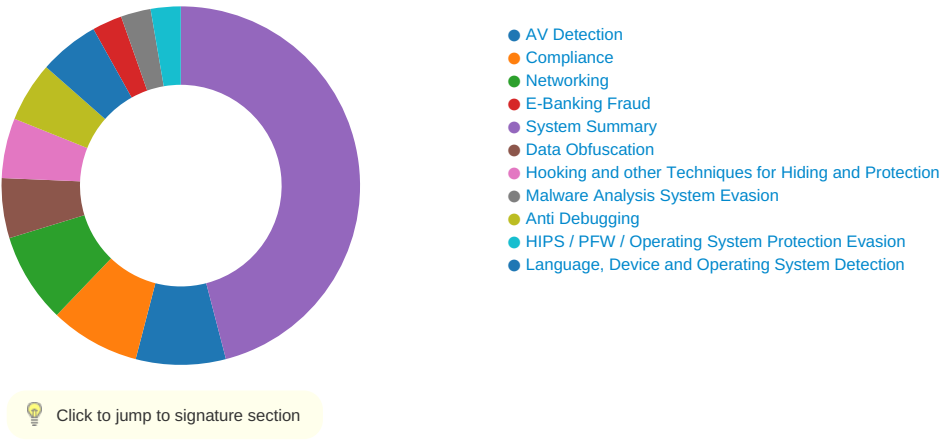
Unpacked PEs

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:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

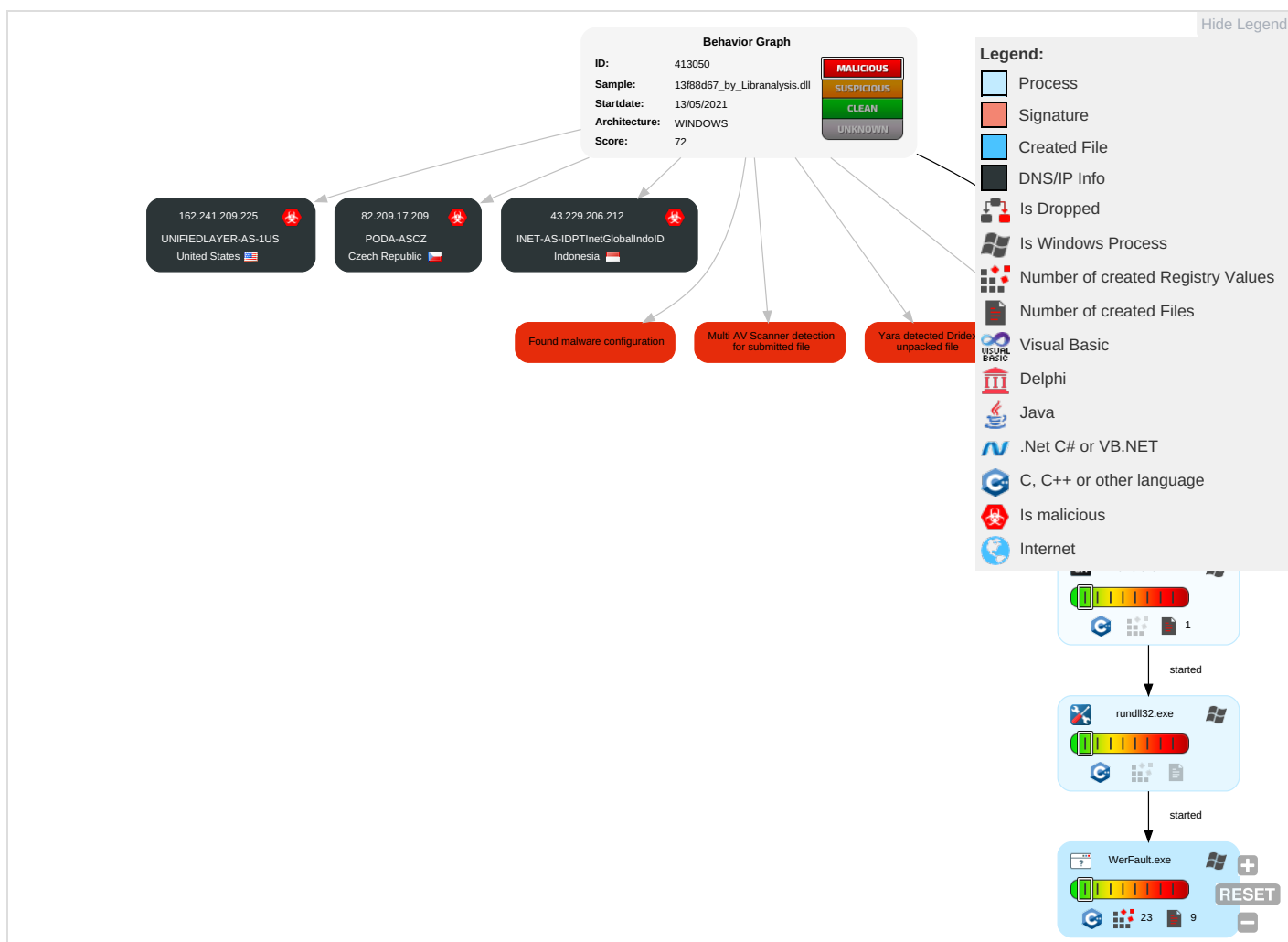
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication

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

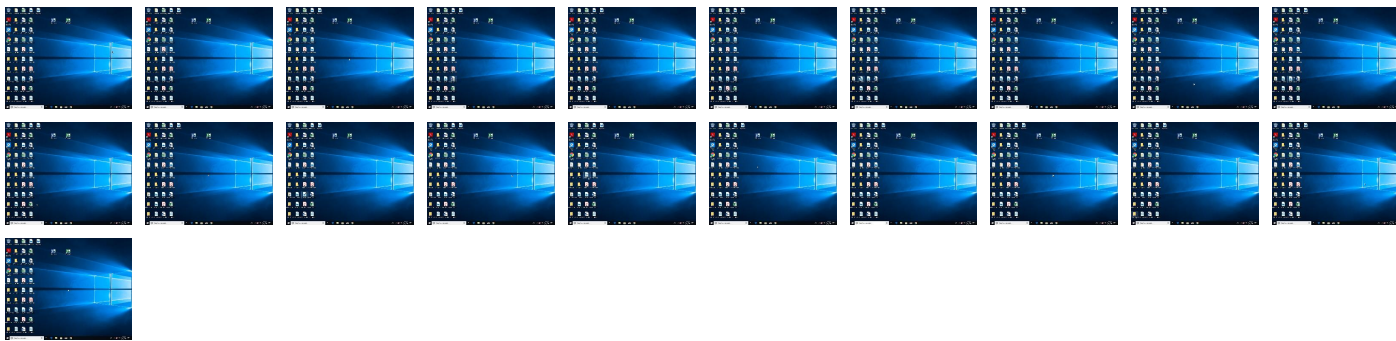
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.
Copyright Joe Security LLC 2021



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
13f88d67_by_Libranalysis.dll	32%	ReversingLabs	Win32.Trojan.Convagent	
13f88d67_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.3150000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

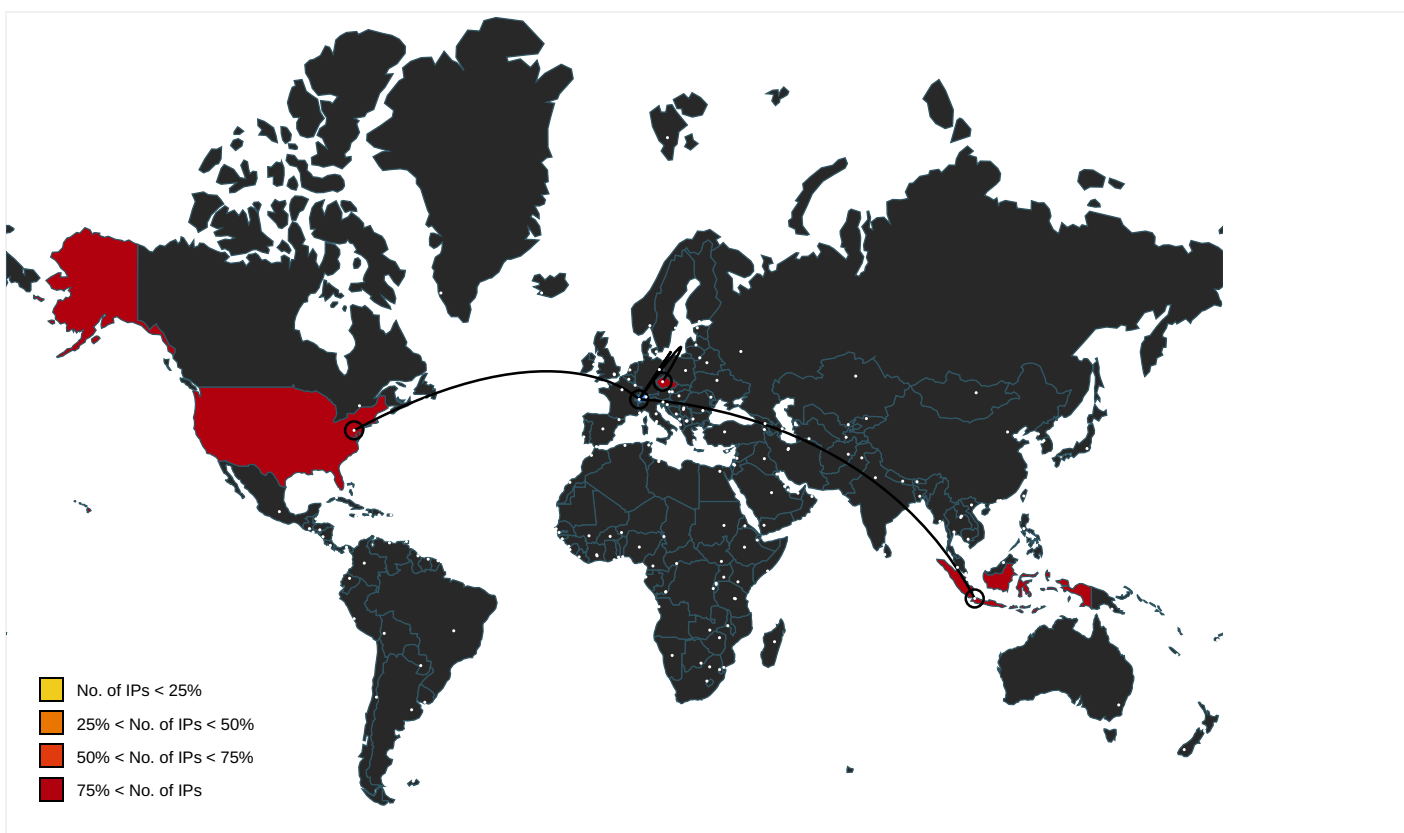
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413050
Start date:	13.05.2021

Start time:	07:09:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	13f88d67_by_Libranalysis.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	23
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: 97.5% (good quality ratio 85.1%) • Quality average: 67.2% • Quality standard deviation: 35%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll • Stop behavior analysis, all processes terminated

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	

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	
162.241.209.225	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a98ab505_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1c640454_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6333f266_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f6f2d53_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	c2b6efb1_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	62badb64_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
UNIFIEDLAYER-AS-1US	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225

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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_4cf7ab5a3fac6be1759bd2786b0f31a62b2a732_82810a17_1a1822e2\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12478
Entropy (8bit):	3.768309050603101
Encrypted:	false
SSDEEP:	192:dsi40oX4cHBUZMX4jed+eG/u7sQS274ItWcP:yi+XTBUZMX4jei/u7sQX4ItWcP
MD5:	F0CBE9930FAFE12D6693DDBB2CDB8342
SHA1:	8E957380DDB8C244C5BD856D6F54E3DE0C5EC2F7
SHA-256:	801D62D506C173DF8243DFA12BE0327C72AF15E9100B8BD014A3FBF4CB4D0A74
SHA-512:	18E43AED9803CD9B571324637E3F3F278EC3AEE78516E5E7A7665872B03FAB761CD8D77370F65510556374405E983EED1B2D5D1DC12949A1B4789BEB15A8A5A
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.=1.3.2.6.5.3.5.6.2.6.7.9.0.6.2.7.1.7.....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.=1.3.2.6.5.3.5.6.2.7.5.1.5.6.2.5.5.4.....R.e.p.o.r.t.S.t.a.t.u.s.=2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=8.3.e.5.5.f.3.9.-.6.3.f.b.-.4.b.a.5.-.b.7.e.2.-.3.0.b.9.a.c.8.0.5.b.8.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=9.d.1.5.4.f.2.d.-.b.6.a.0.-.4.9.f.7.-.9.b.b.4.-.9.f.d.a.9.f.e.0.a.6.3.1.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.1.b.4.0.-.0.0.0.1.-.0.0.1.b.-.c.1.0.3.-.c.5.4.d.b.6.4.7.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.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\WER78B.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe

C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8294
Entropy (8bit):	3.698455694249005
Encrypted:	false
SSDEEP:	192:RrI7r3GLNiM686YSw6p0gmfTbVSpFhFx+pr289bA6sfkgm:RrlsNiw686Y96p0gmfTBSCAZfy
MD5:	EC6D24E7F5D863476F68307E93C1582B
SHA1:	A8961673614EA90734094EC78E8A295A05C170C4
SHA-256:	4711B208B74F8E54064C35C94D8659C84AE347CE9A5DE0B52A9DCD688F57B8E8
SHA-512:	A19E480AC2F7E30C8490BDF5346C35116EE0C3BAFF397F18BBDD44FB8472E447D0CDFC20802DB2501DF9D0678744E961B9419ED5D583BDE06F6602C52E473AF
Malicious:	false
Reputation:	low
Preview:	..<?x.m.l..v.e.r.s.i.o.n.="1..0"..e.n.c.o.d.i.n.g.="U.T.F.-1.6"?.>.....<W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0..0.</W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<B.u.i.l.d.>1.7.1.3.4.</B.u.i.l.d.>.....<P.r.o.d.u.c.t>.(0.x.3.0).. W.i.n.d.o.w.s..1.0..P.r.o.</P.r.o.d.u.c.t>.....<E.d.i.t.i.o.n.>P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n.>.....<B.u.i.l.d.S.t.r.i.n.g.>1.7.1.3.4..1...a.m.d.6.4.f.r.e..r.s.4..r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.</B.u.i.l.d.S.t.r.i.n.g.>.....<R.e.v.i.s.i.o.n.>1.</R.e.v.i.s.i.o.n.>.....<F.l.a.v.o.r.>M.u.l.t.i.p.r.o.c.e.s.s.o.r..F.r.e.e.</F.l.a.v.o.r.>.....<A.r.c.h.i.t.e.c.t.u.r.e.>X.6.4.</A.r.c.h.i.t.e.c.t.u.r.e.>.....<L.C.I.D.>1.0.3.3.</L.C.I.D.>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<P.i.d.>6.9.7.6.</P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7.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):	4.476195904908416
Encrypted:	false
SSDEEP:	48:cvlwSD8zsTrJgtWI9c6WSC8B08fm8M4JCdsNNrFj+q8/INFan4SrS1d:uITTFz7SNDJnN9XNUndW1d
MD5:	114A43520E6EB0F3EAD92931408CBB31
SHA1:	ABCB72704239A9AE03568BFD7F8453007C13C86E
SHA-256:	74663C61E9D82889D2C999648A39A560C699EEE23F72903D0C06EBCD9E944559
SHA-512:	12A47F0C133B203A4D9DFDB25AEFC1C9053EF34B384CCAD5B63D9D024BA18FCEE89A6F3BC561390B3211D35804C724D61F430463A7DB9DC4FDF78FDBFD3B477
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">..<tlm>..<src>..<desc>..<mach>..<os>..<arg nm="vermaj" val="10" />..<arg nm="vermin" val="0" />..<arg nm="verbld" val="17134" />..<arg nm="vercsdbld" val="1" />..<arg nm="verqfe" val="1" />..<arg nm="csdbld" val="1" />..<arg nm="versp" val="0" />..<arg nm="arch" val="9" />..<arg nm="lcid" val="1033" />..<arg nm="geoid" val="244" />..<arg nm="sku" val="48" />..<arg nm="domain" val="0" />..<arg nm="prodsuite" val="256" />..<arg nm="ntprodtype" val="1" />..<arg nm="platid" val="2" />..<arg nm="tmsi" val="987261" />..<arg nm="osinsty" val="1" />..<arg nm="iever" val="11.1.17134.0-1.0.47" />..<arg nm="portos" val="0" />..<arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEC0.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 05:11:09 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	53158
Entropy (8bit):	2.0287399140043743
Encrypted:	false
SSDEEP:	192:MnwXFcyzMeTBwtPdcmKJufdun4npZpXSpjpdPPOz3zvsXyop4t3Ybn3Ho:UyL8e/MdFICp1d+v6p4mY
MD5:	F3B35E0497AD9EE8C79B8753ABCD485E
SHA1:	4362F820631D6B6B12B3CA3A6BFEC5730065CED4
SHA-256:	EFBE314C816E4610BE4C4D3AA41AC8CC4F24DA8777531661E2D9A266AD3B23CE
SHA-512:	EB7592923A6646735A816FDC7ADCD86C843B2307C5D511B67D7C510914470E76E7CDBE380CF6999DA32376A1B9BD0264AA8A84C05C6DDDE86443CC6016D5D62
Malicious:	false
Reputation:	low
Preview:	MDMP.....`.....U.....B.....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.....

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.513887471369652
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:	13f88d67_by_Libranalysis.dll
File size:	167424
MD5:	13f88d6731bf769d9690cbc0f1009697
SHA1:	6f3536a9dde8f77dd031eb6e88a8b296c00a5f44
SHA256:	3a6248e07dc73d8a3d543ac8e1f31c15c643af735b17bc30329facb3c6043a02
SHA512:	de281f76d5aca2b46b0218f7a5fc167bcd13e5502b0591bc2cef4830f44af9ef76c19cdbbbea416ad1625c511e56fac16c84e9b16d40c9d093ece289beba60
SSDEEP:	3072:R9F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:R9F6rQXvFczyYpQP
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.Xm.o...< ...<...<U!<...<..B<r...<...<rQ!<...<...<...<3..<au.<...< szt"<...<Rich...<.....

File Icon	
	
Icon Hash:	74f0e4eccdce0e4

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:	0x609C7F97 [Thu May 13 01:23:35 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	88962f6760ea005847fb88b87e8ce1fd

Entrypoint Preview

Instruction
mov eax, 00000000h
cmpss xmm1, xmm2, 03h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp eax, 02h
mov eax, ebp

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

Resources

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

Imports

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

Version Infos

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:10:27.274174929 CEST	65298	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:27.322946072 CEST	53	65298	8.8.8.8	192.168.2.4
May 13, 2021 07:10:27.521486998 CEST	59123	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:27.580260038 CEST	53	59123	8.8.8.8	192.168.2.4
May 13, 2021 07:10:28.080286026 CEST	54531	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:28.137336969 CEST	53	54531	8.8.8.8	192.168.2.4
May 13, 2021 07:10:29.023421049 CEST	49714	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:29.074980021 CEST	53	49714	8.8.8.8	192.168.2.4
May 13, 2021 07:10:29.497720003 CEST	58028	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:29.556791067 CEST	53	58028	8.8.8.8	192.168.2.4
May 13, 2021 07:10:29.915229082 CEST	53097	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:29.974467039 CEST	53	53097	8.8.8.8	192.168.2.4
May 13, 2021 07:10:30.844408989 CEST	49257	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:30.893577099 CEST	53	49257	8.8.8.8	192.168.2.4
May 13, 2021 07:10:32.310713053 CEST	62389	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:10:32.362446070 CEST	53	62389	8.8.8.8	192.168.2.4
May 13, 2021 07:10:33.144855976 CEST	49910	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:33.196604967 CEST	53	49910	8.8.8.8	192.168.2.4
May 13, 2021 07:10:33.952194929 CEST	55854	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:34.003633022 CEST	53	55854	8.8.8.8	192.168.2.4
May 13, 2021 07:10:34.998660088 CEST	64549	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:35.050117016 CEST	53	64549	8.8.8.8	192.168.2.4
May 13, 2021 07:10:36.060074091 CEST	63153	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:36.109755039 CEST	53	63153	8.8.8.8	192.168.2.4
May 13, 2021 07:10:37.045898914 CEST	52991	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:37.098819017 CEST	53	52991	8.8.8.8	192.168.2.4
May 13, 2021 07:10:40.615593910 CEST	53700	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:40.664247990 CEST	53	53700	8.8.8.8	192.168.2.4
May 13, 2021 07:10:42.273535967 CEST	51726	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:42.322691917 CEST	53	51726	8.8.8.8	192.168.2.4
May 13, 2021 07:10:43.373672962 CEST	56794	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:43.422414064 CEST	53	56794	8.8.8.8	192.168.2.4
May 13, 2021 07:10:44.894807100 CEST	56534	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:44.946223974 CEST	53	56534	8.8.8.8	192.168.2.4
May 13, 2021 07:10:46.462462902 CEST	56627	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:46.511141062 CEST	53	56627	8.8.8.8	192.168.2.4
May 13, 2021 07:10:47.264036894 CEST	56621	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:47.314100981 CEST	53	56621	8.8.8.8	192.168.2.4
May 13, 2021 07:10:48.143296957 CEST	63116	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:48.203038931 CEST	53	63116	8.8.8.8	192.168.2.4
May 13, 2021 07:10:49.525072098 CEST	64078	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:49.573765993 CEST	53	64078	8.8.8.8	192.168.2.4
May 13, 2021 07:10:59.608259916 CEST	64801	53	192.168.2.4	8.8.8.8
May 13, 2021 07:10:59.665498018 CEST	53	64801	8.8.8.8	192.168.2.4
May 13, 2021 07:11:12.050704002 CEST	61721	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:12.107681990 CEST	53	61721	8.8.8.8	192.168.2.4
May 13, 2021 07:11:15.629429102 CEST	51255	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:15.679850101 CEST	53	51255	8.8.8.8	192.168.2.4
May 13, 2021 07:11:21.305963039 CEST	61522	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:21.366127968 CEST	53	61522	8.8.8.8	192.168.2.4
May 13, 2021 07:11:29.701179028 CEST	52337	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:29.761332035 CEST	53	52337	8.8.8.8	192.168.2.4
May 13, 2021 07:11:30.552367926 CEST	55046	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:30.612159014 CEST	53	55046	8.8.8.8	192.168.2.4
May 13, 2021 07:11:31.168103933 CEST	49612	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:31.225336075 CEST	53	49612	8.8.8.8	192.168.2.4
May 13, 2021 07:11:31.645741940 CEST	49285	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:31.702888012 CEST	53	49285	8.8.8.8	192.168.2.4
May 13, 2021 07:11:31.938704014 CEST	50601	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:32.004050970 CEST	53	50601	8.8.8.8	192.168.2.4
May 13, 2021 07:11:32.298957109 CEST	60875	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:32.360143900 CEST	53	60875	8.8.8.8	192.168.2.4
May 13, 2021 07:11:32.893227100 CEST	56448	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:32.943706036 CEST	53	56448	8.8.8.8	192.168.2.4
May 13, 2021 07:11:33.386832952 CEST	59172	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:33.443845034 CEST	53	59172	8.8.8.8	192.168.2.4
May 13, 2021 07:11:34.150532961 CEST	62420	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:34.212058067 CEST	53	62420	8.8.8.8	192.168.2.4
May 13, 2021 07:11:35.709364891 CEST	60579	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:35.766309977 CEST	53	60579	8.8.8.8	192.168.2.4
May 13, 2021 07:11:36.244266033 CEST	50183	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:36.292980909 CEST	53	50183	8.8.8.8	192.168.2.4
May 13, 2021 07:11:36.955794096 CEST	61531	53	192.168.2.4	8.8.8.8
May 13, 2021 07:11:37.014770031 CEST	53	61531	8.8.8.8	192.168.2.4
May 13, 2021 07:12:18.540571928 CEST	49228	53	192.168.2.4	8.8.8.8
May 13, 2021 07:12:18.589205980 CEST	53	49228	8.8.8.8	192.168.2.4
May 13, 2021 07:12:20.441293001 CEST	59794	53	192.168.2.4	8.8.8.8
May 13, 2021 07:12:20.498544931 CEST	53	59794	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



- loadll32.exe
- cmd.exe
- rundll32.exe
- WerFault.exe



Click to jump to process

System Behavior

Analysis Process: loadll32.exe PID: 6944 Parent PID: 6072

General

Start time:	07:10:33
Start date:	13/05/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\13f88d67_by_Libranalysis.dll'
Imagebase:	0xc30000
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: 6960 Parent PID: 6944

General

Start time:	07:10:34
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\13f88d67_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: 6976 Parent PID: 6960

General

Start time:	07:10:34
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\13f88d67_by_Libranalysis.dll',#1
Imagebase:	0xcc0000
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: 00000002.00000002.760132699.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6744 Parent PID: 6976

General

Start time:	07:11:04
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6976 -s 764
Imagebase:	0x1010000
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
-----------	--------	------------	---------	------------	-------	----------------	--------

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\WERFEC0.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\WERFEC0.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\WER78B.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\WER78B.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\WERAE7.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\WERAE7.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_4cf7ab5a3fac6be1759bd2786b0f31a62b2a732_82810a17_1a1822e2	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_4cf7ab5a3fac6be1759bd2786b0f31a62b2a732_82810a17_1a1822e2\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\WERFEC0.tmp	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7.tmp	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEC0.tmp.dmp	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAE7.tmp.xml	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD6.tmp.csv	success or wait	1	6F564BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREFD.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\WERFEC0.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 ed b4 9c 60 a4 05 12 00 00 00 00 00	MDMP.....`.....	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEC0.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	6F56497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEC0.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 cc 07 00 00 05 00 00 00 24 01 00 00 a8 33 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 8e b1 00 00 15 00 00 00 ec 01 00 00 54 1d 00 00 16 00 00 00 98 00 00 00 40 1f 00 00	\$. ...3.....T.....8..... ...T..... ..T.....@...	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<O.S.V.e.r.s.i.o.n.I.n.f.o.r. m.a.t.i.o.n.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 39 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.9.7.6.</.P.i.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 37 00 30 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.5.7.0.9.<./U.p.t.i.m.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 38 00 32 00 33 00 38 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.8.2.3.8.7.2.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 38 00 31 00 35 00 36 00 38 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.8.1.5.6.8.0.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 39 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.6.9.5.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 35 00 34 00 35 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.>.9.1.5.4.5.6.0.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 31 00 35 00 34 00 35 00 36 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.>.9.1.5.4.5.6.0.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 39 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.2.9.9.4.4.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 36 00 37 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>.2.9.6.7.2.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 38 00 37 00 33 00 36 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.i.e.U.s.a.g.e>.5.8.7.3.6.6.4.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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 38 00 31 00 38 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.8.1.8.5.6.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 38 00 37 00 33 00 36 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.>.5.8.7.3.6.6.4.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 39 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.9.6.0.<./P.i.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 30 00 36 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e>.3.6.0.6.7.<./U.p.t.i.m.e>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 32 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.>.1.1.2.2.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 33 00 31 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.3.1.4.5.6.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 35 00 36 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.4.8.5.6.9.6.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 39 00 32 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.5.9.2.9.6.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 32 00 36 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.1.2.6.7.2.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 39 00 32 00 39 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.5.9.2.9.6.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 74 00 76 00 63 00 62 00 78 00 62 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.>.t.v.c.b.x.b.,.l.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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 74 00 76 00 63 00 62 00 78 00 62 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>.t.v.c.b.x.b.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 33 00 39 00 38 00 39 00 34 00 35 00 34 00 2e 00 42 00 36 00 34 00 2e 00 31 00 39 00 30 00 36 00 31 00 39 00 30 00 35 00 33 00 38 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<.B.I.O.S.V.e.r.s.i.o.n>.V.M.W.7.1...0.0.V...1.3.9.8.9.4.5.4...B.6.4...1.9.0.6.1.9.0.5.3.8.<./B.I.O.S.V.e.r.s.i.o.n>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 39 00 33 00 31 00 30 00 31 00 31 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>.1.5.6.9.3.1.0.1.1.1.<./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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 35 00 3a 00 31 00 31 00 3a 00 31 00 30 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.= ".2.0. 2.1.-.0.5.-.1.3.T.0.5.:.1.1.: 1.0.Z.">	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 39 00 37 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 38 00 35 00 36 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 38 00 35 00 36 00 32 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.l.d.= ".3.6.9". .P.I.D.= ".6.9.7.6". .U.p.t.i.m.e.M.S.= ".2.8.5.6.2". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".2.8.5.6.2". .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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 33 00 65 00 35 00 35 00 66 00 33 00 39 00 2d 00 36 00 33 00 66 00 62 00 2d 00 34 00 62 00 61 00 35 00 2d 00 62 00 37 00 65 00 32 00 2d 00 33 00 30 00 62 00 39 00 61 00 63 00 38 00 30 00 35 00 62 00 38 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.8.3.e.5.5.f.3.9.-.6.3.f.b.-.4.b.a.5.-.b.7.e.2.-.3.0.b.9.a.c.8.0.5.b.8.3.<./G.u.i.d.>.	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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 35 00 3a 00 31 00 31 00 3a 00 31 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.0.5.:.1.1.:.1.0.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WER78B.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER78B.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\WERAE7.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_4cf7ab5a3fac6be1759bd2786b0f31a62b2a732_82810a17_1a1822e2\Report.wer	unknown	2	ff fe	..	success or wait	1	6F56497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_4cf7ab5a3fac6be1759bd2786b0f31a62b2a732_82810a17_1a1822e2\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_4cf7ab5a3fac6be1759bd2786b0f31a62b2a732_82810a17_1a1822e2\Report.wer	unknown	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 35 00 31 00 36 00 38 00 37 00 34 00 34 00 38 00	M.e.t.a.d.a.t.a.H.a.s.h.=.- .5.1.6.8.7.4.4.8.	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\{351a1acd-7044-7e33-8309-4d3b4b390afb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5836BF	unknown
\REGISTRYA\{351a1acd-7044-7e33-8309-4d3b4b390afb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5836BF	unknown
\REGISTRYA\{351a1acd-7044-7e33-8309-4d3b4b390afb}\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\{351a1acd-7044-7e33-8309-4d3b4b390afb}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5643D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{351a1acd-7044-7e33-8309-4d3b4b390afb}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6F5836BF	unknown
\REGISTRYA\{351a1acd-7044-7e33-8309-4d3b4b390afb}\Root\InventoryApplicationFile\rundll32.exe ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6F5836BF	unknown

