

JOeSandbox Cloud BASIC



ID: 413065

Sample Name:

2fba2168_by_Libranalysis

Cookbook: default.jbs

Time: 07:25:07

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 2fba2168_by_Libranalysis	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Dridex	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Networking:	5
E-Banking Fraud:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
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	12
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	16
Statistics	17
Behavior	17
System Behavior	17
Analysis Process: loadll32.exe PID: 6164 Parent PID: 5656	17
General	17
File Activities	17
Analysis Process: cmd.exe PID: 6172 Parent PID: 6164	17
General	17
File Activities	18
Analysis Process: rundll32.exe PID: 6184 Parent PID: 6172	18
General	18
Analysis Process: WerFault.exe PID: 7096 Parent PID: 6184	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 2fba2168_by_Libranalysis

Overview

General Information

Sample Name:

2fba2168_by_Libranalysis
(renamed file extension from none to dll)

Analysis ID:

413065

MD5:

2fba21684f9cee9..

SHA1:

c4d402963878c1..

SHA256:

f6521a28e0d4f21..

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Dridex

Score:

64

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

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...

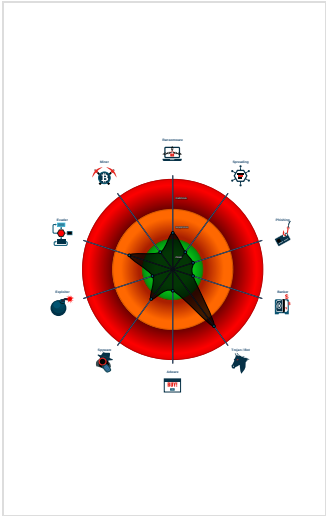
Detected potential crypto function

IP address seen in connection with o...

Internet Provider seen in connection...

Monitors certain registry keys / valu...

Classification



Startup

System is w10x64

loadaddll32.exe (PID: 6164 cmdline: loadaddll32.exe 'C:\Users\user\Desktop\2fba2168_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 6172 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2fba2168_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 6184 cmdline: rundll32.exe 'C:\Users\user\Desktop\2fba2168_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 7096 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6184 -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": [
    "16dkGS0zdHgjuCciXGd5X7UrHwfYsUG8wEUtKNgzHrWMfTGafJbc",
    "39t3NdDhurvp1tFNCpVA5goSy1kxj1BtIwMPTv1DPbNEcuIekQC70"
  ]
}
```

Yara Overview

Memory Dumps

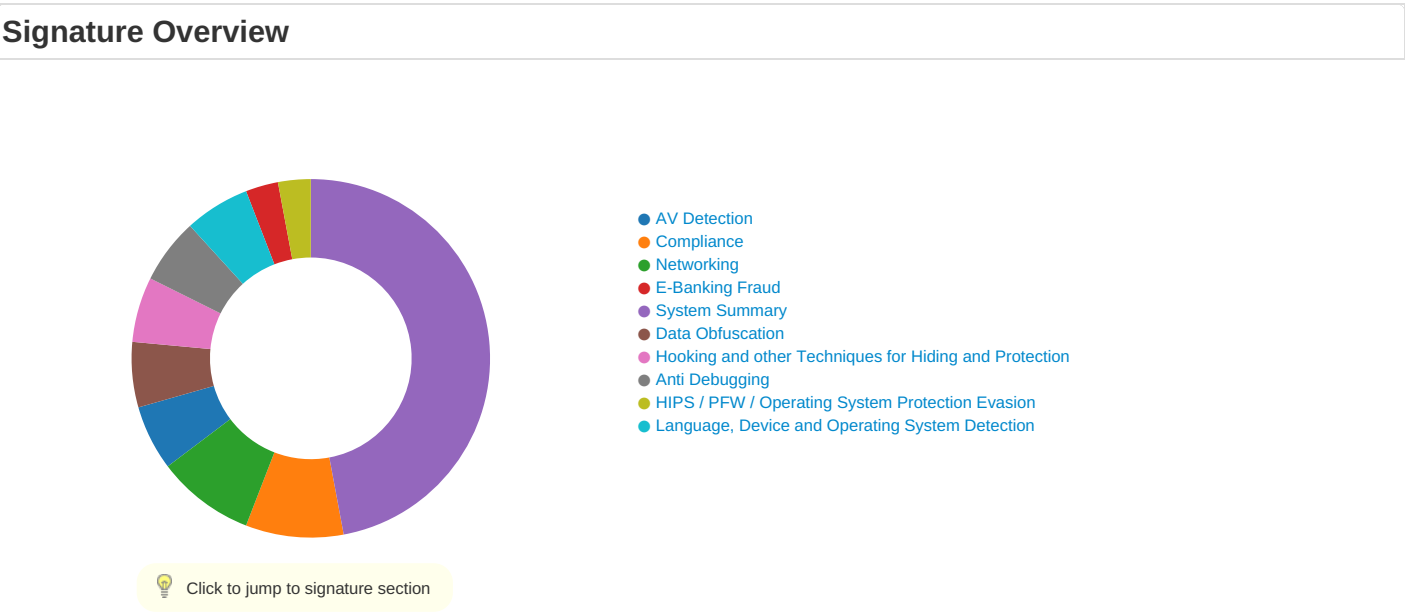
Source	Rule	Description	Author	Strings
00000002.00000002.306535551.0000000010001000.00000020.00020000.sdmf	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

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



AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

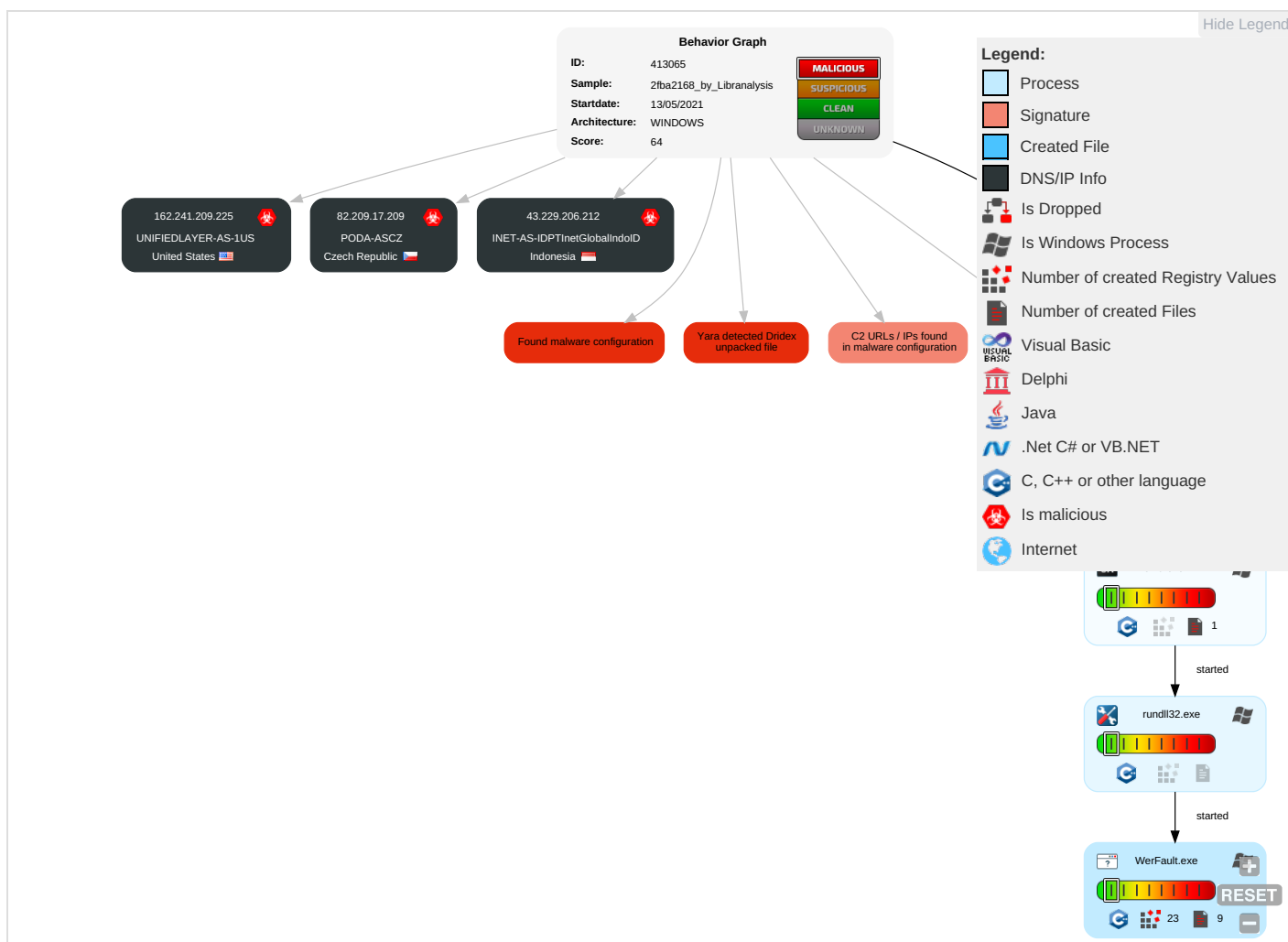
Yara detected Dridex unpacked file

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
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	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Phone Calls/SMS

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

Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
2fba2168_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.2fc0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

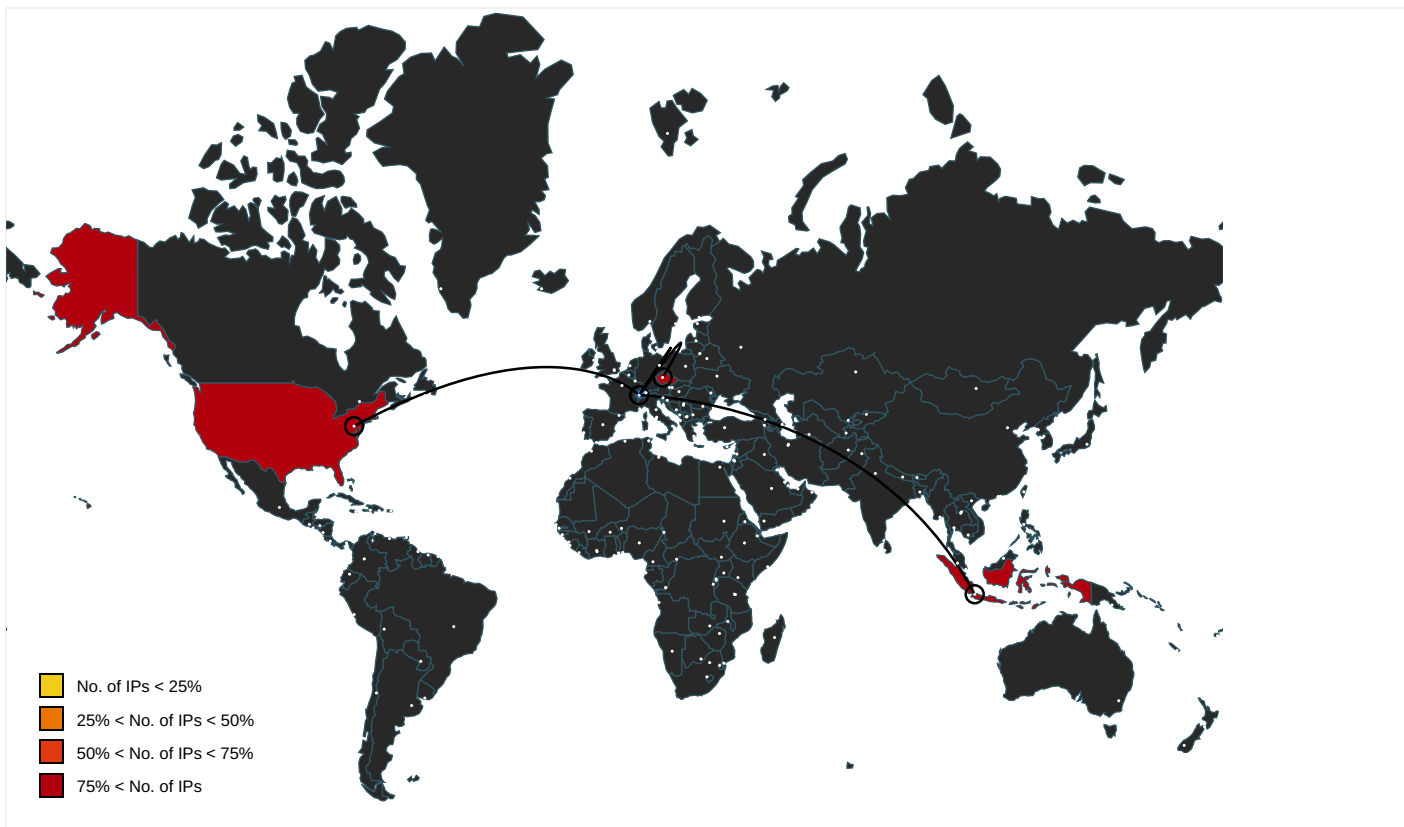
No Antivirus matches

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:	413065
Start date:	13.05.2021
Start time:	07:25:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 46s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	2fba2168_by_Libranalysis (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
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:	mal64.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 57% (good quality ratio 49.4%) • Quality average: 67.4% • Quality standard deviation: 35.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Simulations

Behavior and APIs

Time	Type	Description
07:26:43	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.209.225	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	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
UNIFIEDLAYER-AS-1US	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	162.241.209.225

C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp.dmp	
SHA-256:	50BC0172E643A896F0CEC48AA9F223B3FF47682B3E50CC8652415D869C0F613E
SHA-512:	D038D38374E319A415287F0F0C2EA70DF71B3AC7A069CCA70D336FB4A4CFE0601C8AC7FDA2D94FC4C16E9480C61DBA481AE99EFAFA14C1BF4839ABF7579AC1A
Malicious:	false
Reputation:	low
Preview:	MDMP..... 7.`.....U.....B.....GenuineIntelW.....T.....(.....6.`.....0.=.....P.a.c.i.f.i.c..S.t.a.n.d.a.r.d..T.i.m.e.....P.a.c.i.f.i.c..D.a.y.l.i.g.h.t..T.i.m.e.....1.7.1.3.4..1...x.8.6.f.r.e...r.s.4..._r.e.l.e.a.s.e...1.8.0.4.1.0.-1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,1.0...0..1.7.1.3.4..1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8292
Entropy (8bit):	3.694301511766365
Encrypted:	false
SSDEEP:	192:Rr17r3GLNieC6+6Yhs6cgmfTYVSCCprZ89bYaOOksfZlm:RrlsNiz6+6Ya6cgmfT4SMYaXfD
MD5:	1CC39FBC80377E4F7959D4ACDEE173B5
SHA1:	BBA81B3E8395EB5602713CC251BF4BE8AEC6A028
SHA-256:	469B8F6637CF9894359784C035F30ECBE195FC22EBC37E7BA6E7112544267E87
SHA-512:	C250D23BB3C4CD756E40F4F3D6B6CA96A34F066319945996ED0FE704D94EB80C40DD303FDA03B7F39BA462F257163D4588F92EFEB6409B0068CD6F00185112D
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.>(0x3.0);. .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.>6.1.8.4.</P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA556.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):	4.4746475795150475
Encrypted:	false
SSDEEP:	48:cvlwSD8zssJgtWI9GAWSC8BUe8fm8M4JCds+NrFe+q8/HNFv4SrSLd:ulTfqV5SNmbJsNM8N9DWLd
MD5:	6BE5FF421C5789944F82D24DA2BF773F
SHA1:	2F0435BD996A4B6B32737708F087245158ACABD4
SHA-256:	37DBF3F0402A95B01129C4DCC267594D022B3D7260C564CBE8E5AF44B22F9F83
SHA-512:	FA42F3B6C50ADEAC1E6DD02224B186D989422763E6B530989CDD66512F0BE5FAE7F9C4FC96F07242CCB69C56829F5C1CF5BE5BFE5B50D925C2EAD950D3FE510B
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="verblid" 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="987817" />..<arg nm="osinsty" val="1" />..<arg nm="iever" val="11.1.17134.0-1 1.0.47" />..<arg nm="portos" val="0" />..<arg nm="ram" val="4096" />..

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.513878329899262

General

TrID:	- Win32 Dynamic Link Library (generic) (1002004/3) 99.60% - Generic Win/DOS Executable (2004/3) 0.20% - DOS Executable Generic (2002/1) 0.20% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	2fba2168_by_Libranalysis.dll
File size:	167424
MD5:	2fba21684f9cee9e69c81f516fa6f564
SHA1:	c4d402963878c169a6149d7d8f43f85ac7c0c12d
SHA256:	f6521a28e0d4f21ec9d6a59f787d5e6251c2c2146b3141e de44820d3614a5779
SHA512:	dd24bf8760d69ad5f942d1fc84ecd083ac09778783ecacf 656b5e210746a63bb4f77ce7a68a48910a9bb82e1f5feb4 2e4dcabdee823d518142a417e97a1f42ed
SSDEEP:	3072:29F/oNrQb4xVubbbXP/NTccbsFvCeLmXH57V30e 8Pj;29F6rQXvFczvYpQP
File Content Preview:	MZ.....@.....\.....!..L!Th is program cannot be run in DOS mode...\$......Xm.o...< ...<...<U!<...<..B<r...<...<rQ!<...<...<...<3..<au.<...< sz!<...<Rich...<.....

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10024cc0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609C8025 [Thu May 13 01:25:57 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
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp eax, 02h
mov eax, ebp
mov dword ptr [10029734h], eax
mov eax, ebx
```


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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 07:25:57.938117981 CEST	53	50620	8.8.8.8	192.168.2.3
May 13, 2021 07:25:58.090055943 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 07:25:58.165978909 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 07:25:58.673769951 CEST	60152	53	192.168.2.3	8.8.8.8
May 13, 2021 07:25:58.725931883 CEST	53	60152	8.8.8.8	192.168.2.3
May 13, 2021 07:25:59.507867098 CEST	57544	53	192.168.2.3	8.8.8.8
May 13, 2021 07:25:59.561276913 CEST	53	57544	8.8.8.8	192.168.2.3
May 13, 2021 07:26:00.668514013 CEST	55984	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:00.730794907 CEST	53	55984	8.8.8.8	192.168.2.3
May 13, 2021 07:26:00.863681078 CEST	64185	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:00.912404060 CEST	53	64185	8.8.8.8	192.168.2.3
May 13, 2021 07:26:01.683482885 CEST	65110	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:01.732305050 CEST	53	65110	8.8.8.8	192.168.2.3
May 13, 2021 07:26:02.882029057 CEST	58361	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:02.933504105 CEST	53	58361	8.8.8.8	192.168.2.3
May 13, 2021 07:26:03.838167906 CEST	63492	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:03.889414072 CEST	53	63492	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:26:04.731040001 CEST	60831	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:04.782543898 CEST	53	60831	8.8.8.8	192.168.2.3
May 13, 2021 07:26:05.532747984 CEST	60100	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:05.581553936 CEST	53	60100	8.8.8.8	192.168.2.3
May 13, 2021 07:26:07.667964935 CEST	53195	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:07.719585896 CEST	53	53195	8.8.8.8	192.168.2.3
May 13, 2021 07:26:08.513835907 CEST	50141	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:08.562529087 CEST	53	50141	8.8.8.8	192.168.2.3
May 13, 2021 07:26:09.388216019 CEST	53023	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:09.439402103 CEST	53	53023	8.8.8.8	192.168.2.3
May 13, 2021 07:26:10.672744989 CEST	49563	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:10.721647024 CEST	53	49563	8.8.8.8	192.168.2.3
May 13, 2021 07:26:11.529457092 CEST	51352	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:11.578620911 CEST	53	51352	8.8.8.8	192.168.2.3
May 13, 2021 07:26:13.231054068 CEST	59349	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:13.281929970 CEST	53	59349	8.8.8.8	192.168.2.3
May 13, 2021 07:26:14.088349104 CEST	57084	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:14.136991978 CEST	53	57084	8.8.8.8	192.168.2.3
May 13, 2021 07:26:15.292376995 CEST	58823	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:15.342806101 CEST	53	58823	8.8.8.8	192.168.2.3
May 13, 2021 07:26:17.155204058 CEST	57568	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:17.204781055 CEST	53	57568	8.8.8.8	192.168.2.3
May 13, 2021 07:26:25.807163000 CEST	50540	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:25.868737936 CEST	53	50540	8.8.8.8	192.168.2.3
May 13, 2021 07:26:42.161396980 CEST	54366	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:42.218687057 CEST	53	54366	8.8.8.8	192.168.2.3
May 13, 2021 07:26:44.985694885 CEST	53034	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:45.043519020 CEST	53	53034	8.8.8.8	192.168.2.3
May 13, 2021 07:26:53.891522884 CEST	57762	53	192.168.2.3	8.8.8.8
May 13, 2021 07:26:53.950203896 CEST	53	57762	8.8.8.8	192.168.2.3
May 13, 2021 07:27:03.092555046 CEST	55435	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:03.151369095 CEST	53	55435	8.8.8.8	192.168.2.3
May 13, 2021 07:27:30.477190018 CEST	50713	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:30.536890030 CEST	53	50713	8.8.8.8	192.168.2.3
May 13, 2021 07:27:35.632688999 CEST	56132	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:35.689703941 CEST	53	56132	8.8.8.8	192.168.2.3
May 13, 2021 07:27:54.975250006 CEST	58987	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:55.026815891 CEST	53	58987	8.8.8.8	192.168.2.3
May 13, 2021 07:27:55.660052061 CEST	56579	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:55.717127085 CEST	53	56579	8.8.8.8	192.168.2.3
May 13, 2021 07:27:56.314263105 CEST	60633	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:56.371546984 CEST	53	60633	8.8.8.8	192.168.2.3
May 13, 2021 07:27:56.577215910 CEST	61292	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:56.634275913 CEST	53	61292	8.8.8.8	192.168.2.3
May 13, 2021 07:27:57.012459040 CEST	63619	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:57.061223030 CEST	53	63619	8.8.8.8	192.168.2.3
May 13, 2021 07:27:57.612756014 CEST	64938	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:57.664381027 CEST	53	64938	8.8.8.8	192.168.2.3
May 13, 2021 07:27:58.254887104 CEST	61946	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:58.303589106 CEST	53	61946	8.8.8.8	192.168.2.3
May 13, 2021 07:27:58.821774960 CEST	64910	53	192.168.2.3	8.8.8.8
May 13, 2021 07:27:58.883989096 CEST	53	64910	8.8.8.8	192.168.2.3
May 13, 2021 07:28:00.129184008 CEST	52123	53	192.168.2.3	8.8.8.8
May 13, 2021 07:28:00.177917004 CEST	53	52123	8.8.8.8	192.168.2.3
May 13, 2021 07:28:01.266190052 CEST	56130	53	192.168.2.3	8.8.8.8
May 13, 2021 07:28:01.314861059 CEST	53	56130	8.8.8.8	192.168.2.3
May 13, 2021 07:28:01.835982084 CEST	56338	53	192.168.2.3	8.8.8.8
May 13, 2021 07:28:01.885653973 CEST	53	56338	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



● loaddll32.exe
● cmd.exe
● rundll32.exe
● WerFault.exe

💡 Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6164 Parent PID: 5656

General

Start time:	07:26:05
Start date:	13/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\2fba2168_by_Libranalysis.dll'
Imagebase:	0x13d0000
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: 6172 Parent PID: 6164

General

Start time:	07:26:05
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\2fba2168_by_Libranalysis.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes

MD5 hash:	F3DBE3BB6F734E357235F4D5898582D
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: 6184 Parent PID: 6172

General

Start time:	07:26:06
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\2fba2168_by_Libranalysis.dll",#1
Imagebase:	0x180000
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: 00000002.00000002.306535551.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 7096 Parent PID: 6184

General

Start time:	07:26:36
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6184 -s 764
Imagebase:	0xf10000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	702B1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA556.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA556.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3b68747a563f6dc075ce1d8715b428671c2ff110_82810a17_1b84ae1e	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3b68747a563f6dc075ce1d8715b428671c2ff110_82810a17_1b84ae1e\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	702A497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA556.tmp	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp.dmp	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA556.tmp.xml	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER23AD.tmp.csv	success or wait	1	702A4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER23CD.tmp.txt	success or wait	1	702A4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 20 37 9d 60 a4 05 12 00 00 00 00 00	MDMP..... 7.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp	unknown	6	00 00 00 00 00 00		success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	...r.u.n.d.l.l.3.2...e.x.e...	success or wait	51	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp.dmp	unknown	752	00 00 48 74 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 62 25 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 f0 24 02 00 00 00 00 00 80 b1 02 00 00 00 00 19 53 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 45 dd 00 00 00 00 00 00 4e 63 03 00 00 00 00 00 36 b5 02 00 00 00 00 00 ff ff ff 00 00 00 00 7d 16 22 00 00 00 00 00 40 ff 1f 00 00 00 00 00 46 2b 22 00 00 00 00	..Ht....0...U..s@..b%.....B.....B?.....#..... ..@A.....Zb.....\$. ..S.....E.....Nc6.....}. @.....F+.....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	E.v.e.n.t.....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.I.R.T.i.m	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A2.tmp.dmp	unknown	108	03 00 00 00 94 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 9c 07 00 00 05 00 00 00 e4 00 00 00 ac 30 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 fe 97 00 00 15 00 00 00 ec 01 00 00 24 1d 00 00 16 00 00 00 98 00 00 00 10 1f 00 00	0.....T.....8..... ...T..... ..\$.....	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?.x.m.l..v.e.r.s.i.o.n.=." 1...0". .e.n.c.o.d.i.n.g.=." U.T.F.-.1.6."?>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.l.n.f.o.r m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.1.8.4.</.P.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.</.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 34 00 33 00 33 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.4.3.3.1.<./U.p.t.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 32 00 39 00 39 00 35 00 38 00 34 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.>.1.2.7.2.9.9.5.8.4.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 32 00 39 00 31 00 33 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.>.1.2.7.2.9.1.3.9.2.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 37 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.7.0.0.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 30 00 37 00 38 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.0.7.8.0.8.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 39 00 32 00 30 00 37 00 38 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.0.7.8.0.8.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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.I.U.s.a.g.e>.1.8.4.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 33 00 31 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.I.U.s.a.g.e>.3.0.3.1.2.<./Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 30 00 30 00 34 00 30 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.I.U.s.a.g.e>.3.0.0.4.0.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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 32 00 30 00 34 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e>.5.8.2.0.4.1.6.<./P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 32 00 38 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.8.2.8.6.0.8.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 32 00 30 00 34 00 31 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.>.5.8.2.0.4.1.6.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.6.1.7.2.<./P.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.c.m.d...e.x.e.<./I.m.a.g.e.N.a.m.e.>.	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 32 00 32 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<U.p.t.i.m.e>.3.5.2.2.6.<./U.p.t.i.m.e>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<I.p.t.E.n.a.b.l.e.d>.0.<./I.p.t.E.n.a.b.l.e.d>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 36 00 32 00 37 00 38 00 34 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.>.5.7.4.6.2.7.8.4.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 38 00 37 00 31 00 33 00 36 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.>.5.2.1.8.7.1.3.6.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.0.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 38 00 36 00 36 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.8.6.6.6.2.4.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 38 00 32 00 31 00 35 00 36 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.8.2.1.5.6.8.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	<QuotaPeakPage.d.PoolUsage>.4.0.9.6.0.</QuotaPeakPage.d.PoolUsage>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	<QuotaPage.PoolUsage>.3.3.2.1.6.</QuotaPage.PoolUsage>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPage.d.PoolUsage>.5.7.6.8.</QuotaPeakNonPage.d.PoolUsage>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 30 00 38 00 38 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	<QuotaNonPage.d.PoolUsage>.5.0.8.8.</QuotaNonPage.d.PoolUsage>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 34 00 36 00 31 00 36 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.>.2.4.6.1.6.9.6.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 35 00 37 00 31 00 37 00 31 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.>.3.5.7.1.7.1.2.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 34 00 36 00 31 00 36 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.>.2.4.6.1.6.9.6.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<P.a.r.a.m.e.t.e.r.0>.r.u.n.d.l.l.3.2...e.x.e.<./P.a.r.a.m.e.t.e.r.0>.	success or wait	8	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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...2.5.6...4.8.<./P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 78 00 61 00 66 00 61 00 69 00 78 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<.S.y.s.t.e.m.M.a.n.u.f.a.c.t.u.r.e.r.>.x.a.f.a.i.x.,. .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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 78 00 61 00 66 00 61 00 69 00 78 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.x.a.f.a.i.x.7,..1.<./.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 38 00 34 00 36 00 32 00 32 00 37 00 34 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.>.1.5.6.8.4.6.2.2.7.4.<./.O.S.I.n.s.t.a.l.l.D.a.t.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<.T.i.m.e.Z.o.n.e.B.i.a.s.>.0.8.:.0.0.<./T.i.m.e.Z.o.n.e.B.i.a.s.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./F.l.a.g.s.>.	success or wait	3	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 32 00 36 00 3a 00 34 00 31 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.= ".2.0. 2.1.-0.5.-1.3.T.1.4.:2.6:.. 4.1.Z.">	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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 34 00 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 38 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 39 00 35 00 39 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 39 00 35 00 39 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 32 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.= ".3.4.5". .P.I.D.= ".6.1.8.4". .U.p.t.i.m.e.M.S.= ".2.9.5.9.3". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".2.9.5.9.3". .S.u.s.p.e.n.d.e.d.M.S.= ".0". .H.a.n.g.C.o.u.n.t.= ".0". .G.h.o.s.t.C.o.u.n.t.= ".0". .C.r.a.s.h.e.d	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 62 00 35 00 30 00 39 00 35 00 32 00 36 00 2d 00 61 00 65 00 64 00 35 00 2d 00 34 00 32 00 31 00 61 00 2d 00 62 00 31 00 31 00 38 00 2d 00 65 00 63 00 31 00 33 00 39 00 37 00 36 00 37 00 62 00 34 00 30 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.b.b.5.0.9.5.2.6-.a.e.d.5.-.4.2.1.a.-.b.1.1.8-.e.c.1.3.9.7.6.7.b.4.0.c.<./.G.u.i.d.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 32 00 36 00 3a 00 34 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.4.:.2.6.:4.1.Z.<./.C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA19C.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	702A497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA556.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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3b68747a563f6dc075ce1d8715b428671c2ff110_82810a17_1b84ae1e\Report.wer	unknown	2	ff fe	..	success or wait	1	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3b68747a563f6dc075ce1d8715b428671c2ff110_82810a17_1b84ae1e\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	702A497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_3b68747a563f6dc075ce1d8715b428671c2ff110_82810a17_1b84ae1e\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 36 00 31 00 32 00 35 00 37 00 34 00 31 00 32 00 31 00	M.e.t.a.d.a.t.a.H.a.s.h.=.- .6.1.2.5.7.4.1.2.1.	success or wait	1	702A497A	unknown

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRYA\{863e8488-89a6-d8c3-6e65-b4897d4e2e09}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRYA\{863e8488-89a6-d8c3-6e65-b4897d4e2e09}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702C36BF	unknown
\REGISTRYA\{863e8488-89a6-d8c3-6e65-b4897d4e2e09}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	702C36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	702C1FB2	RegCreateKeyExW
\REGISTRYA\{863e8488-89a6-d8c3-6e65-b4897d4e2e09}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	702A43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRYA\{863e8488-89a6-d8c3-6e65-b4897d4e2e09}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519fec486de87ed73cb92d3cac802400000000	success or wait	1	702C36BF	unknown
\REGISTRYA\{863e8488-89a6-d8c3-6e65-b4897d4e2e09}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	702C36BF	unknown

