

JOeSandbox Cloud BASIC



ID: 413063

Sample Name:

e3429d75_by_Libranalysis.dll

Cookbook: default.jbs

Time: 07:28:35

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report e3429d75_by_Libranalysis.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Dridex	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Networking:	5
E-Banking Fraud:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	8
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	10
ASN	11
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	13
General	13
File Icon	14
Static PE Info	14
General	14
Entrypoint Preview	14
Rich Headers	15
Data Directories	15
Sections	15
Resources	16
Imports	16
Version Infos	16
Network Behavior	16

UDP Packets	16
Code Manipulations	17
Statistics	17
Behavior	17
System Behavior	18
Analysis Process: loadll32.exe PID: 5116 Parent PID: 5728	18
General	18
File Activities	18
Analysis Process: cmd.exe PID: 4612 Parent PID: 5116	18
General	18
File Activities	18
Analysis Process: rundll32.exe PID: 2268 Parent PID: 4612	18
General	18
Analysis Process: WerFault.exe PID: 6312 Parent PID: 2268	19
General	19
File Activities	19
File Created	19
File Deleted	19
File Written	20
Registry Activities	42
Key Created	42
Key Value Created	42
Disassembly	43
Code Analysis	43

Analysis Report e3429d75_by_Libranalysis.dll

Overview

General Information

Sample Name:

e3429d75_by_Libranalysis.dll

Analysis ID:

413063

MD5:

e3429d75f100410.

SHA1:

eb96ff932b65254..

SHA256:

b5c92ef90ff138e...

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Dridex

Score:

72

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected Dridex unpacked file

C2 URLs / IPs found in malware con...

Machine Learning detection for samp...

Checks if the current process is bein...

Contains functionality to check if a d...

Contains functionality to query locale...

Creates a DirectInput object (often fo...

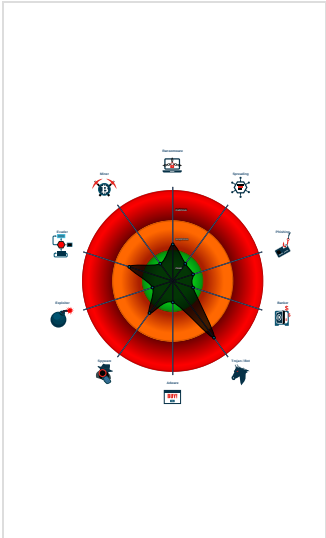
Creates a process in suspended mo...

Detected potential crypto function

IP address seen in connection with o...

Internet Provider seen in connection...

Classification



Startup

System is w10x64

loadll32.exe (PID: 5116 cmdline: loadll32.exe 'C:\Users\user\Desktop\le3429d75_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 4612 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\le3429d75_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 2268 cmdline: rundll32.exe 'C:\Users\user\Desktop\le3429d75_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 6312 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2268 -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": [

"16dkGSt0zdHgjuCciXGdSX7UrHkfYSUG8wEUtKNgzHrWMfTGafJbC",

"39t3NdDhurvp1tFNCpva5goSylkxjIBtIwHPTv1DPbNEcuIekQC70"

]

}

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.325708369.0000000010001000.0000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

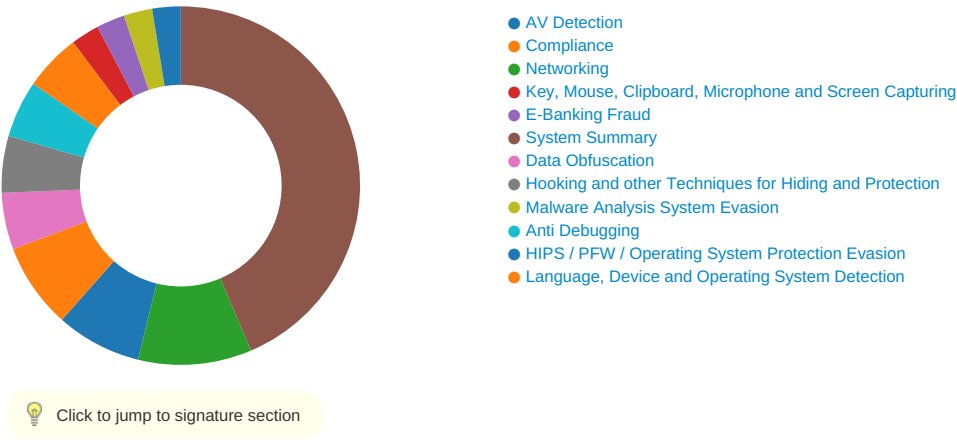
Unpacked PEs

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

Sigma Overview

No Sigma rule has matched

Signature Overview



AV Detection:

Found malware configuration
Multi AV Scanner detection for submitted file
Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration
--

E-Banking Fraud:

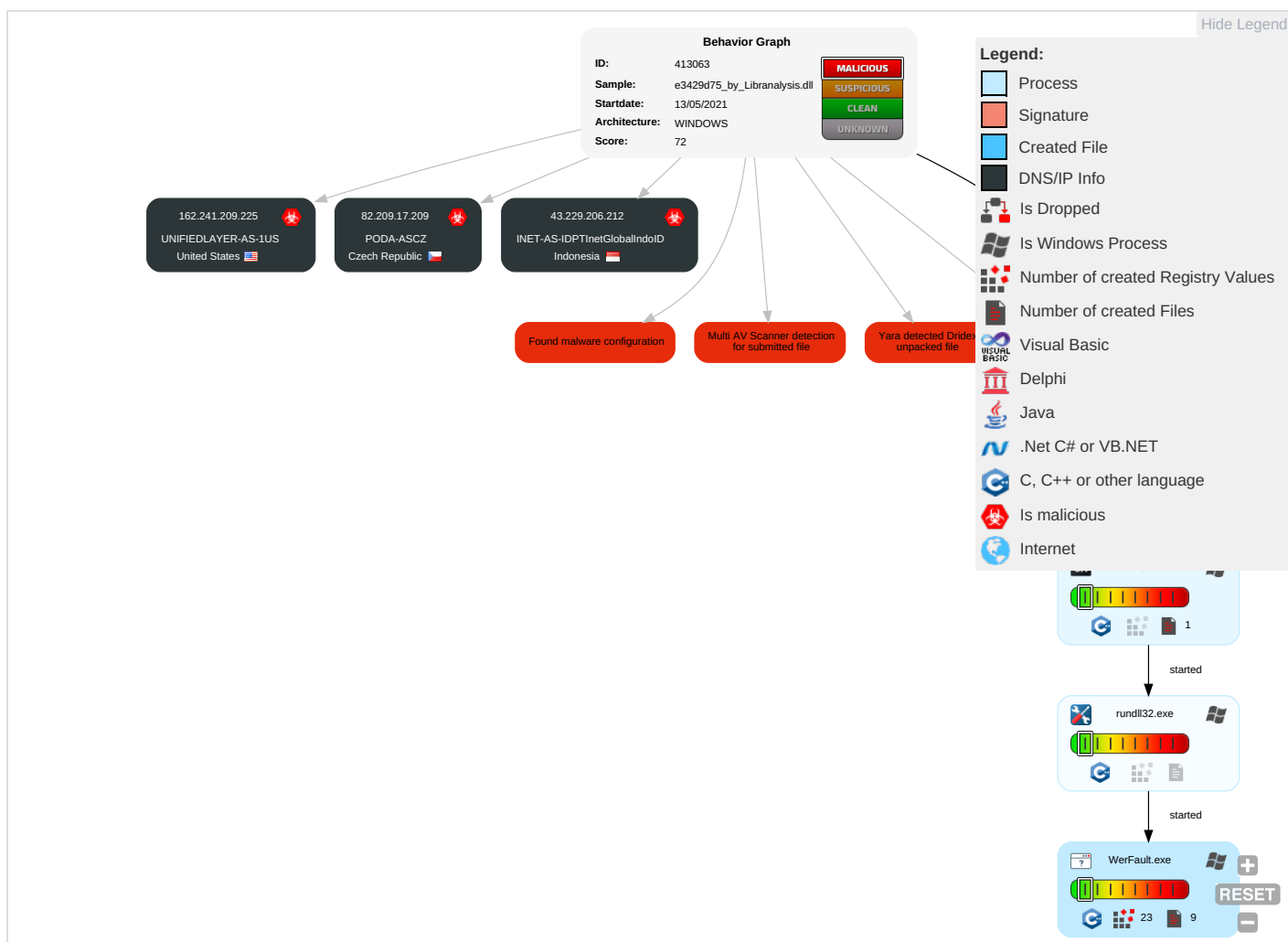
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati

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

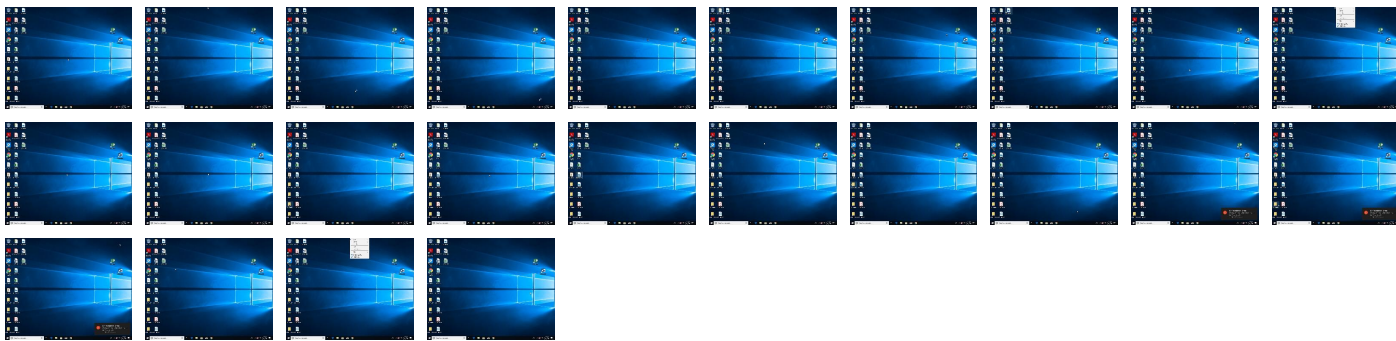
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
e3429d75_by_Libranalysis.dll	36%	ReversingLabs	Win32.Trojan.Convagent	
e3429d75_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.2890000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.microsoft.c	0%	URL Reputation	safe	
http://www.microsoft.c	0%	URL Reputation	safe	
http://www.microsoft.c	0%	URL Reputation	safe	
http://www.microsoft.c	0%	URL Reputation	safe	

Domains and IPs

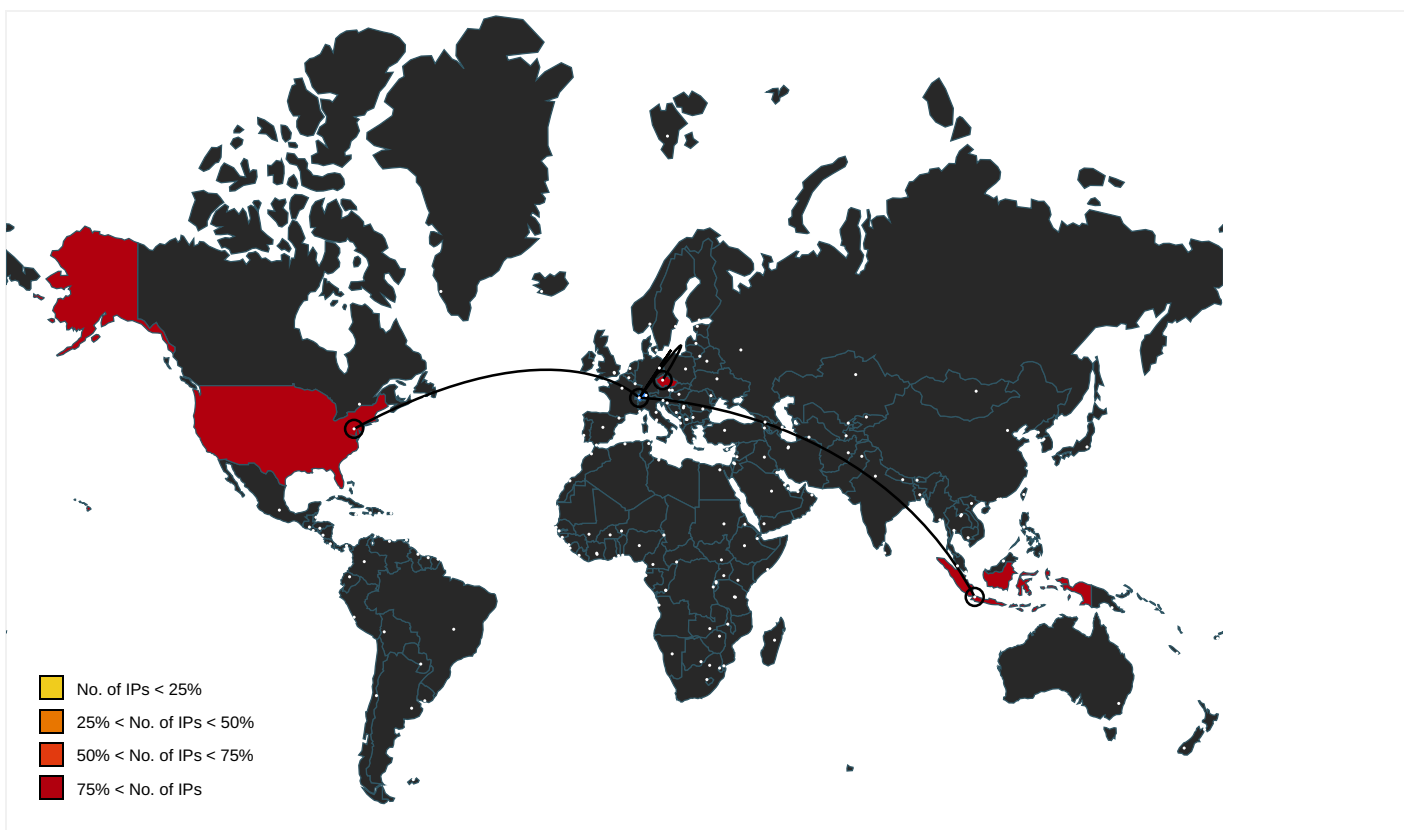
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.microsoft.c	WerFault.exe, 0000000D.0000000 3.319780043.00000000034EE000.0 0000004.00000001.sdmp	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown

Contacted IPs



Public

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

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413063
Start date:	13.05.2021
Start time:	07:28:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	e3429d75_by_Libranalysis.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	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:	mal72.troj.winDLL@6/4@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.7% (good quality ratio 85.3%) • Quality average: 67.2% • Quality standard deviation: 35%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	
162.241.209.225	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	
43.229.206.212	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	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	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PODA-ASCZ	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	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
INET-AS-IDPTInetGlobalIndoID	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
UNIFIEDLAYER-AS-1US	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	e0eb0cb2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	2fba2168_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	1cc57949_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	7587f225_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	e3429d75_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	8b521700_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225

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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_18fa5a08\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12486
Entropy (8bit):	3.766401090919624
Encrypted:	false
SSDEEP:	192:+YX7iI0oXPbcHBUZMX4jed+MO/u7slS274ItWcG:97iuXPYBUZMX4jeQ/u7slX4ItWcG
MD5:	1889FC78B50D18082377A708A0FF0B85
SHA1:	5277575482C296F2E50125C63A5F479FCF8EBA2B
SHA-256:	99A65A5C261B9DF032515ECFA84DE3B13B01D5262B7E502D8B03B5366AD9CB74
SHA-512:	7106F8AC978C24C9003CCCA328B4AF72A1560181DA0A7B94CFADC1FFC58822557FB7109A2E403F1C6DC66E6E5A8088F071893412A24569F0AC6ED084F84F3EE
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=1.....E.v.e.n.t.T.y.p.e.=A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=1.3.2.6.5.3.8.9.8.0.6.7.6.1.3.0.4.6.....R.e.p.o.r.t.T.y.p.e.=2.....C.o.n.s.e.n.t.=1.....U.p.l.o.a.d.T.i.m.e.=1.3.2.6.5.3.8.9.8.1.3.3.2.3.7.9.3.4.....R.e.p.o.r.t.S.t.a.t.u.s.=2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=c.1.3.2.f.d.6.6.-7.4.f.1.-4.8.8.1.-9.1.0.d.-2.b.9.4.f.5.8.c.6.e.1.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=1.2.9.6.7.d.0.8.-4.9.f.9.-4.8.4.7.-9.3.a.c.-5.5.e.e.a.0.0.7.e.6.0.6.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.8.d.c.-0.0.0.1.-0.0.1.6.-8.0.c.2.-a.e.6.7.0.4.4.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.l.d.=W.:0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu May 13 14:30:08 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	48822
Entropy (8bit):	2.0385557976476933
Encrypted:	false
SSDEEP:	192:3e719utZRhhPimGrbpgew+eaZOoDMnjH+H4IFHZKB2eXBwKwEnfe:3U9utHzimgTU2QnjHExa2eXyzEfe
MD5:	FC640A3DA2181FC371EE5A4D2EE4FD9C
SHA1:	F147E549A9F7EB27D8FC4FE5FD7C8DD0111530B6
SHA-256:	E1E6336884F5314020E0CC4630F1400A3941C04F3721B317DC0113E05347C5FD
SHA-512:	59C1CD5349887C6738AE2BBB0B7D22F1DE5BFBCFB2B1221C07CA48C600787D64AE3D04839DDD4EF2533DF658D7A6BB7100D1931977AF724FACF2210785A500
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.tmp.dmp	
Preview:	MDMP.....7.`.....U.....B.....GenuineIntelW.....T.....7.`.....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.....17.1.34..1...x.8.6.f.r.e...r.s.4..._r.e.l.e.a.s.e...18.0.4.1.0.-18.0.4.....d.b.g.c.o.r.e...i.3.8.6.,1.0..0..17.1.34..1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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):	3.6965482131401495
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiTz6rn16YSp6dgmftVVSOcpru89binQsfkoWm:RrlsNiN656YE6dgmftfSxinjFT
MD5:	D551F94B33ACD6935DAE07E13843B2DA
SHA1:	ACE9C8EE0FB2A9435841CEA730B6F29E7367EDB6
SHA-256:	257248CA8BF5253DC727D4AAB837A41926E536A96C49E4622C140A64FBF21E66
SHA-512:	BB3765D303A982561BFF6510B89668AFF79B6B926765AE61E884B5E7BE69FE87E71173CEB21961CC35A45344512E8D4640C7F20DC8234EE2AE4C112EB4999380
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.>17.1.34.</B.u.i.l.d.>.....<P.r.o.d.u.c.t.>(0.x.3.0):. W.i.n.d.o.w.s..1.0..P.r.o. </P.r.o.d.u.c.t.>.....<E.d.i.t.i.o.n.>P.r.o.f.e.s.s.i.o.n.a.l.</E.d.i.t.i.o.n.>.....<B.u.i.l.d.S.t.r.i.n.g.>17.1.34..1...a.m.d.6.4.f.r.e...r.s.4..._r.e.l.e.a.s.e...18.0.4.1.0.-18.0.4. </B.u.i.l.d.S.t.r.i.n.g.>.....<R.e.v.i.s.i.o.n.>1.</R.e.v.i.s.i.o.n.>.....<F.l.a.v.o.r.>M.u.l.t.i.p.r.o.c.e.s.s.o.r..F.r.e.e.</F.l.a.v.o.r.>.....<A.r.c.h.i.t.e.c.t.u.r.e.>X.6.4.</ A.r.c.h.i.t.e.c.t.u.r.e.>.....<L.C.I.D.>1.0.3.3.</L.C.I.D.>.....</O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<P.i.d.>2.2.6.8.</P.i. d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4394.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):	4.472483077656305
Encrypted:	false
SSDEEP:	48:cvlwSD8zsuJgtWi9saWSC8BA8fm8M4JCdsXNrFzQ+q8/6NF24rSVd:uITfkXbSNTJtNGdNMDWVd
MD5:	D76D3C7C22880B79400B059735423D89
SHA1:	F2DFCB2048D9FAE8209C108E483213CE70E70FAE
SHA-256:	E602DCCE447FB9AFD5BD71318932930E7AA34E454C28F77D659A00AAA5C19BA5
SHA-512:	354BBF1876B2BF0EB15B17D9BB7128E0787C01698345666189907D82FA856280DB2286ECF42315FC01C46C509325BB1CDB2C8DACD22F538C3C06B302E5C6CFF
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" >.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" >.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="987820" />.. <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 Wi ndows
Entropy (8bit):	7.513848167670934
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:	e3429d75_by_Libranalysis.dll
File size:	167424
MD5:	e3429d75f100410819a57b3b7ce51aa7
SHA1:	eb96ff932b65254b8de87d09f9e892049f0473a8

General	
SHA256:	b5c92ef90ff138ee8edecb4250170ca12bd1e0b1fcdc58527121bea0f104b504
SHA512:	d8145cf3397f8eae35ed14c6f895dcf278e16b8a92c1d345325909225ce2c9dbcd08befe720f43d54c025858c999aec531603206616f710ecc6aec3dfeff6e3
SSDEEP:	3072:h9F/oNrQb4xVubbxP/NTccbsFvCeLmXH57V30e8Pj:h9F6rQXvFczyYpQP
File Content Preview:	MZ.....@.....\.....!..L!Th is program cannot be run in DOS mode...\$.....Xm.o...< ...<...<.U!<...<..B<r...<...<...<rQ!<...<...<...<.3..<au.<...< szt<".<Rich...<.....

File Icon

	
Icon Hash:	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:	0x609C8024 [Thu May 13 01:25:56 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	88962f6760ea005847fb88b87e8ce1fd

Entrypoint Preview

Instruction
mov eax, 00000000h
cmpss xmm1, xmm2, 03h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp eax, 02h
mov eax, ebp
mov dword ptr [10029734h], eax
mov eax, ebx
mov dword ptr [10029730h], eax
mov eax, esi
mov dword ptr [10029728h], eax
jne 00007F4E4CCBA326h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

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

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2770a	0x5b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x277d8	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x1220	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x10018	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x25000	0x4c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x23e44	0x23e00	False	0.756362968206	data	7.53078515147	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x25000	0x2a04	0x2c00	False	0.753728693182	data	7.42331753213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crt	0x28000	0x34d0	0x1800	False	0.79052734375	MMDF mailbox	7.46423038313	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x3a0	0x400	False	0.4248046875	data	3.06187161643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x26c	0x400	False	0.548828125	data	4.2946697642	IMAGE_SCN_TYPE_NOLOAD, IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_TYPE_NO_PAD, IMAGE_SCN_TYPE_GROUP, IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Version Infos

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:29:32.066432953 CEST	54795	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:32.123461008 CEST	53	54795	8.8.8.8	192.168.2.5
May 13, 2021 07:29:32.882455111 CEST	49557	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:32.931303978 CEST	53	49557	8.8.8.8	192.168.2.5
May 13, 2021 07:29:34.242989063 CEST	61733	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:34.291898966 CEST	53	61733	8.8.8.8	192.168.2.5
May 13, 2021 07:29:35.018101931 CEST	65447	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:35.069739103 CEST	53	65447	8.8.8.8	192.168.2.5
May 13, 2021 07:29:35.925538063 CEST	52441	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:35.977030039 CEST	53	52441	8.8.8.8	192.168.2.5
May 13, 2021 07:29:37.457165003 CEST	62176	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:37.505671978 CEST	53	62176	8.8.8.8	192.168.2.5
May 13, 2021 07:29:38.254934072 CEST	59596	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:38.311822891 CEST	53	59596	8.8.8.8	192.168.2.5
May 13, 2021 07:29:39.168864965 CEST	65296	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:39.220437050 CEST	53	65296	8.8.8.8	192.168.2.5
May 13, 2021 07:29:42.141961098 CEST	63183	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:42.193584919 CEST	53	63183	8.8.8.8	192.168.2.5
May 13, 2021 07:29:42.925025940 CEST	60151	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:42.976774931 CEST	53	60151	8.8.8.8	192.168.2.5
May 13, 2021 07:29:49.553415060 CEST	56969	53	192.168.2.5	8.8.8.8
May 13, 2021 07:29:49.612705946 CEST	53	56969	8.8.8.8	192.168.2.5
May 13, 2021 07:30:13.443068027 CEST	55161	53	192.168.2.5	8.8.8.8
May 13, 2021 07:30:13.503010988 CEST	53	55161	8.8.8.8	192.168.2.5
May 13, 2021 07:30:14.115137100 CEST	54757	53	192.168.2.5	8.8.8.8
May 13, 2021 07:30:14.164432049 CEST	53	54757	8.8.8.8	192.168.2.5
May 13, 2021 07:30:23.354625940 CEST	49992	53	192.168.2.5	8.8.8.8
May 13, 2021 07:30:23.415859938 CEST	53	49992	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:30:25.971399069 CEST	60075	53	192.168.2.5	8.8.8.8
May 13, 2021 07:30:26.031712055 CEST	53	60075	8.8.8.8	192.168.2.5
May 13, 2021 07:30:55.393160105 CEST	55016	53	192.168.2.5	8.8.8.8
May 13, 2021 07:30:55.450594902 CEST	53	55016	8.8.8.8	192.168.2.5
May 13, 2021 07:30:58.043195963 CEST	64345	53	192.168.2.5	8.8.8.8
May 13, 2021 07:30:58.100507021 CEST	53	64345	8.8.8.8	192.168.2.5
May 13, 2021 07:31:16.767544031 CEST	57128	53	192.168.2.5	8.8.8.8
May 13, 2021 07:31:16.833317995 CEST	53	57128	8.8.8.8	192.168.2.5
May 13, 2021 07:31:37.520983934 CEST	54791	53	192.168.2.5	8.8.8.8
May 13, 2021 07:31:37.594157934 CEST	53	54791	8.8.8.8	192.168.2.5
May 13, 2021 07:31:39.463694096 CEST	50463	53	192.168.2.5	8.8.8.8
May 13, 2021 07:31:39.525413036 CEST	53	50463	8.8.8.8	192.168.2.5
May 13, 2021 07:32:06.206631899 CEST	50394	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:06.306426048 CEST	53	50394	8.8.8.8	192.168.2.5
May 13, 2021 07:32:06.938739061 CEST	58530	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:07.051706076 CEST	53	58530	8.8.8.8	192.168.2.5
May 13, 2021 07:32:07.874733925 CEST	53813	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:07.934762955 CEST	53	53813	8.8.8.8	192.168.2.5
May 13, 2021 07:32:08.503751040 CEST	63732	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:08.566318989 CEST	53	63732	8.8.8.8	192.168.2.5
May 13, 2021 07:32:09.553019047 CEST	57344	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:09.611027956 CEST	53	57344	8.8.8.8	192.168.2.5
May 13, 2021 07:32:10.654541016 CEST	54450	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:10.712234974 CEST	53	54450	8.8.8.8	192.168.2.5
May 13, 2021 07:32:12.164079905 CEST	59261	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:12.221273899 CEST	53	59261	8.8.8.8	192.168.2.5
May 13, 2021 07:32:13.841583967 CEST	57151	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:13.890399933 CEST	53	57151	8.8.8.8	192.168.2.5
May 13, 2021 07:32:14.889350891 CEST	59413	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:14.938158035 CEST	53	59413	8.8.8.8	192.168.2.5
May 13, 2021 07:32:15.556075096 CEST	60516	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:15.604760885 CEST	53	60516	8.8.8.8	192.168.2.5
May 13, 2021 07:32:20.738868952 CEST	51649	53	192.168.2.5	8.8.8.8
May 13, 2021 07:32:20.803836107 CEST	53	51649	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loadll32.exe PID: 5116 Parent PID: 5728

General

Start time:	07:29:38
Start date:	13/05/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\le3429d75_by_Libranalysis.dll'
Imagebase:	0x9f0000
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: 4612 Parent PID: 5116

General

Start time:	07:29:38
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\le3429d75_by_Libranalysis.dll',#1
Imagebase:	0xfa0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Analysis Process: rundll32.exe PID: 2268 Parent PID: 4612

General

Start time:	07:29:38
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\le3429d75_by_Libranalysis.dll',#1
Imagebase:	0x830000
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: 00000002.00000002.325708369.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6312 Parent PID: 2268

General

Start time:	07:30:04
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2268 -s 764
Imagebase:	0x1070000
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	6D9D1717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	read attributes generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4394.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4394.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_18fa5a08	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_18fa5a08\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D9C497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.tmp	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4394.tmp	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.tmp.dmp	success or wait	1	6D9C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	success or wait	1	6D9C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4394.tmp.xml	success or wait	1	6D9C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER43C0.tmp.csv	success or wait	1	6D9C4BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AF5.tmp.txt	success or wait	1	6D9C4BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.tmp.dmp	unknown	32	4d 44 4d 50 93 a7 ee a0 0e 00 00 00 20 00 00 00 00 00 00 00 f0 37 9d 60 a4 05 12 00 00 00 00 00	MDMP.....7.`.....	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.tmp.dmp	unknown	6	00 00 00 00 00 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.tmp.dmp	unknown	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 ee 42 00 00 02 00 00 00 a8 1f 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 ff fb 8b 1f 00 00 00 00 54 05 00 00 f7 03 00 00 dc 08 00 00 d2 37 9d 60 07 00 00 00 10 00 00 00 93 08 00 00 93 08 00 00 93 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 3d 00 00 00 00 00 00 00 02 00 00 00 e0 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	U.....B..... ..GenuineIntelW.....T...7.`.....0..=..... P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T. i.m.e.....	success or wait	1	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3902.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 9e a0 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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.O.S.V.e.r.s.i.o.n.I.n.f.o.r. m.a.t.i.o.n>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 39 00 37 00 38 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.>.2.9.7.8.1.<./U.p.t.i.m.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 31 00 31 00 39 00 30 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.>.9.2.1.1.9.0.4.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 31 00 31 00 39 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.1.1.9.0.4.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.1.8.4.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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.l.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.l.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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.l.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.l.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 37 00 39 00 31 00 37 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.7.9.1.7.4.4.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 37 00 39 00 39 00 39 00 33 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s. a.g.e.>.5.7.9.9.3.6. <./P.e. a.k.P.a.g.e.f.i.l.e.U.s.a.g.e. >.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 37 00 39 00 31 00 37 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5. 7.9.1.7.4.4.<./P.r.i.v.a.t.e. U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 34 00 36 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.4.6.1.2.<./P.i.d.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 30 00 31 00 30 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e>.3.0.1.0.7.<./U.p.t.i.m.e>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 37 00 34 00 30 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.5.7.4.0.5.4.4.0.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 33 00 34 00 34 00 30 00 35 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.3.4.4.0.5.1.2.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 31 00 32 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.1.1.2.2.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 37 00 32 00 37 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.2.7.3.6.0.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 37 00 31 00 35 00 30 00 37 00 32 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.>.3.7.1.5.0.7.2.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.4.0.9.6.0.<./Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.3.3.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.6.3.2.<./Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.5.2.2.4.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 33 00 35 00 38 00 38 00 30 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.>.3.5.8.8.0.9.6.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 39 00 36 00 32 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.5.9.6.2.8.8.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 33 00 35 00 38 00 38 00 30 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.>.3.5.8.8.0.9.6.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...0...2.5.6...4.8.<./P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<S.y.s.t.e.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 76 00 6b 00 68 00 64 00 6c 00 76 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.>.v.k.h.d.l.v.,.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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 76 00 6b 00 68 00 64 00 6c 00 76 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>.v.k.h.d.l.v.7.,.1.</.S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 35 00 39 00 33 00 39 00 39 00 39 00 36 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e>.1.5.5.9.3.9.9.6.3.</.O.S.I.n.s.t.a.l.l.D.a.t.e>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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.<./F.l.a.g.s.>.	success or wait	3	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 33 00 30 00 3a 00 30 00 38 00 5a 00 22 00 3e 00	<P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.="2.0. 2.1-.0.5-.1.3.T.1.4.:3.0.: 0.8.Z.">.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	266	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 33 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 32 00 36 00 38 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 35 00 30 00 34 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 35 00 30 00 34 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<P.r.o.c.e.s.s. .A.s.I.d.="3.3.6". .P.I.D.="2.2.6.8". .U.p.t.i.m.e.M.S.="2.5.0.4.6". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.="2.5.0.4.6". .S.u.s.p.e.n.d.e.d.M.S.="0". .H.a.n.g.C.o.u.n.t.="0". .G.h.o.s.t.C.o.u.n.t.="0". .C.r.a.s.h.e.d	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.i.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 31 00 33 00 32 00 66 00 64 00 36 00 36 00 2d 00 37 00 34 00 66 00 31 00 2d 00 34 00 38 00 38 00 31 00 2d 00 39 00 31 00 30 00 64 00 2d 00 32 00 62 00 39 00 34 00 66 00 35 00 38 00 63 00 36 00 65 00 31 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.c.1.3.2.f.d.6.6.-.7.4.f.1.-.4.8.8.1.-.9.1.0.d.-.2.b.9.4.f.5.8.c.6.e.1.c.<./G.u.i.d.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 33 00 30 00 3a 00 30 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.4.:3.0.:0.8.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./R.e.p.o.r.t.i.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FAB.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	6D9C497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4394.tmp.xml	unknown	4663	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>.<req ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_18fa5a08\Report.wer	unknown	2	ff fe	..	success or wait	1	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_18fa5a08\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	6D9C497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_18fa5a08\Report.wer	unknown	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 32 00 39 00 37 00 31 00 31 00 30 00 34 00 30 00 33 00	M.e.t.a.d.a.t.a.H.a.s.h.=.- .1.2.9.7.1.1.0.4.0.3.	success or wait	1	6D9C497A	unknown

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{e0500e3b-85f4-31a3-c817-bc7d72b0037c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9E36BF	unknown
\REGISTRY\A\{e0500e3b-85f4-31a3-c817-bc7d72b0037c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9E36BF	unknown
\REGISTRY\A\{e0500e3b-85f4-31a3-c817-bc7d72b0037c}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D9E36BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D9E1FB2	RegCreateKeyExW
\REGISTRY\A\{e0500e3b-85f4-31a3-c817-bc7d72b0037c}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D9C43D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{e0500e3b-85f4-31a3-c817-bc7d72b0037c}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519fec486de87ed73cb92d3cac802400000000	success or wait	1	6D9E36BF	unknown
\REGISTRY\A\{e0500e3b-85f4-31a3-c817-bc7d72b0037c}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D9E36BF	unknown

