

JOeSandbox Cloud BASIC



ID: 413063

Sample Name:

e3429d75_by_Libranalysis

Cookbook: default.jbs

Time: 07:20:47

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

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

Code Manipulations	17
Statistics	17
Behavior	17
System Behavior	17
Analysis Process: loadll32.exe PID: 4584 Parent PID: 5708	17
General	17
File Activities	18
Analysis Process: cmd.exe PID: 2172 Parent PID: 4584	18
General	18
File Activities	18
Analysis Process: rundll32.exe PID: 5676 Parent PID: 2172	18
General	18
Analysis Process: WerFault.exe PID: 6892 Parent PID: 5676	18
General	19
File Activities	19
File Created	19
File Deleted	19
File Written	19
Registry Activities	41
Key Created	41
Key Value Created	41
Disassembly	42
Code Analysis	42

Analysis Report e3429d75_by_Libranalysis

Overview

General Information

Sample Name:

e3429d75_by_Libranalysis
(renamed file extension from none to 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...

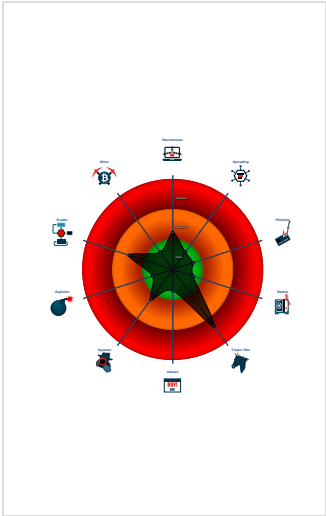
Creates a process in suspended mo...

Detected potential crypto function

IP address seen in connection with o...

Internet Provider seen in connection...

Classification



Startup

System is w10x64

loadall32.exe (PID: 4584 cmdline: loadall32.exe 'C:\Users\user\Desktop\3429d75_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

cmd.exe (PID: 2172 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\3429d75_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

rundll32.exe (PID: 5676 cmdline: rundll32.exe 'C:\Users\user\Desktop\3429d75_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

WerFault.exe (PID: 6892 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5676 -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": [

"16dkGS0zdHgjuCcixGd5X7UrHwHfY5UG8wEUtKNgzHrWMfTGafJbc",

"39t3NdDhurvp1tFNCpva5goSy1kxj1BtIwMPTv1DPbNEcuIekQC70"

]

]

}

Yara Overview

Memory Dumps

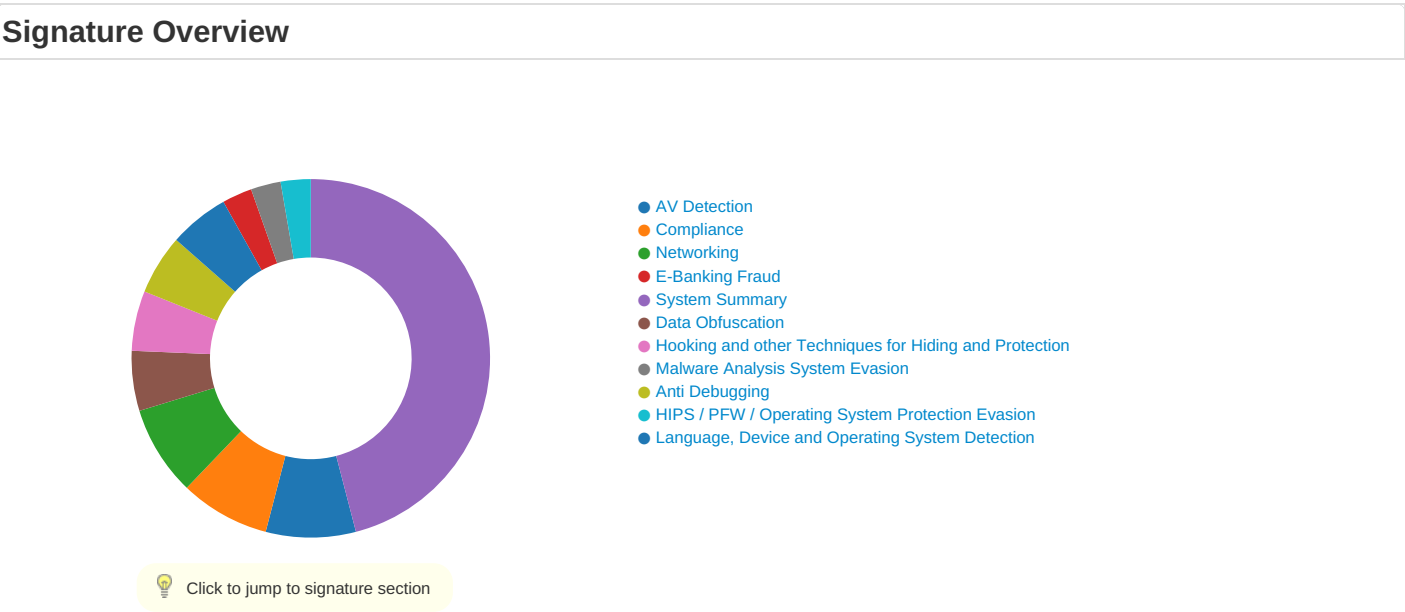
Source	Rule	Description	Author	Strings
00000002.00000002.338342680.0000000010001000.00000020.00020000.sdmf	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

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

Sigma Overview

No Sigma rule has matched



AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

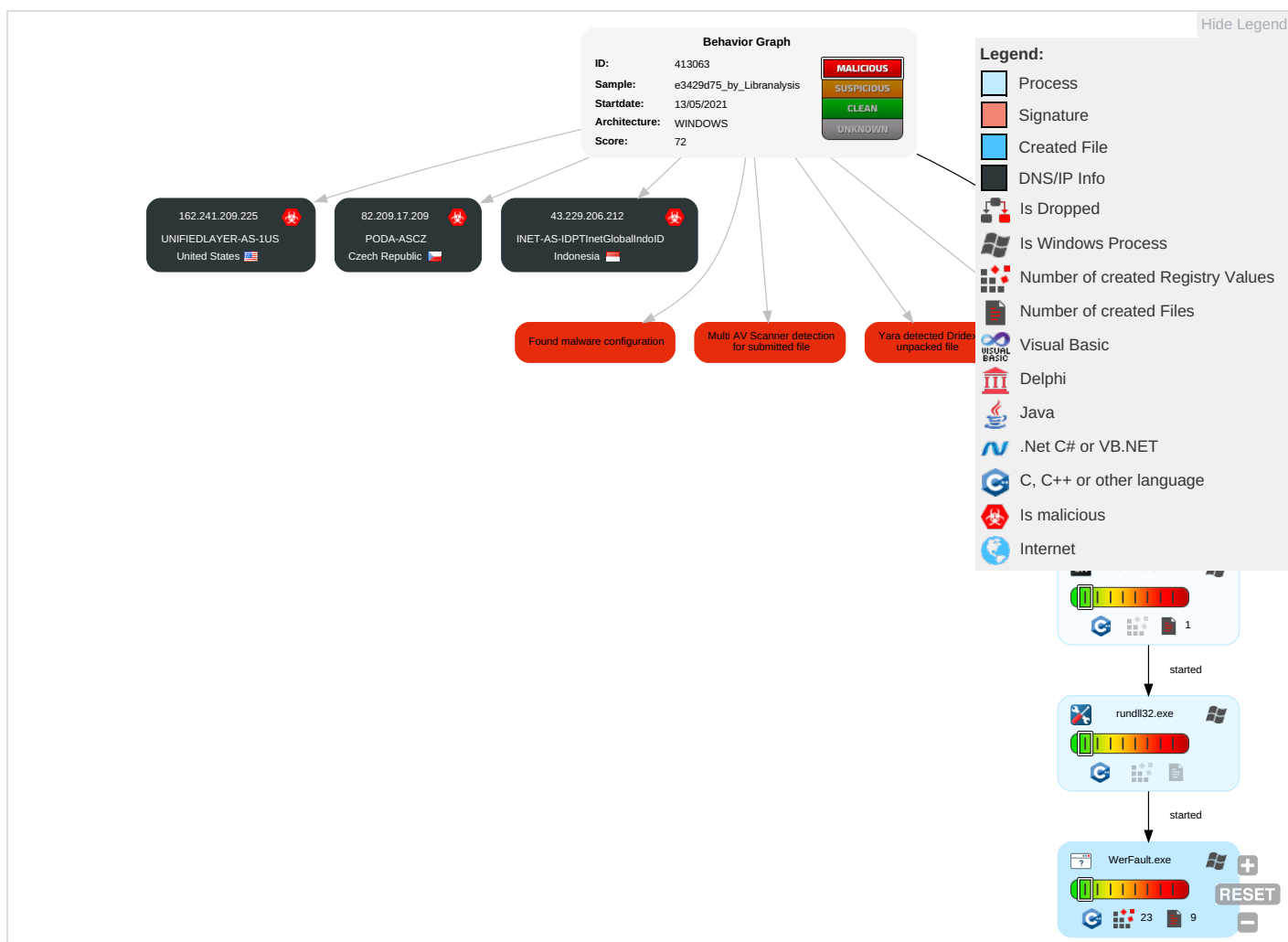
Yara detected Dridex unpacked file

Mitre Att&ck Matrix

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

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

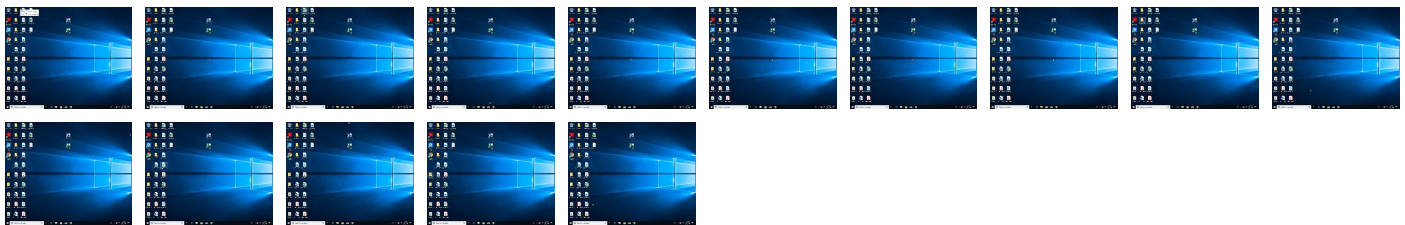
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
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.32b0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413063
Start date:	13.05.2021
Start time:	07:20:47
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	e3429d75_by_Libranalysis (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	33
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: 56.9% (good quality ratio 49.2%) • Quality average: 67.3% • Quality standard deviation: 35.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Simulations

Behavior and APIs

Time	Type	Description
07:22:24	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
82.209.17.209	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
162.241.209.225	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	
43.229.206.212	94a4d66c_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	

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
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	2a71d07d_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	4bfaad72_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	82.209.17.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 82.209.17.209
INET-AS-IDPTInetGlobalIndoID	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
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 43.229.206.212
	5322b76c_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
	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
	0f72be74_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	cdc733ac_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
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	13f88d67_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
	a194019c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	cdc733ac_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	4e021da2_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	27c06d28_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	86fa0c16_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	6bea48e8_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	13f88d67_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	052a78c5_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	fe1d4238_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225
	5322b76c_by_Libranalysis.dll	Get hash	malicious	Browse	• 162.241.20 9.225

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_1abacc56\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	12490
Entropy (8bit):	3.7667834809637335
Encrypted:	false
SSDEEP:	192:Nci9o0oXHbcHBUZMX4jed+1G/u7stS274ltWcK:yi8XHYBUZMX4jep/u7stX4ltWcK
MD5:	629688FEB3584A2579F11FECDB0E48E4
SHA1:	77858A2143FFD2C00E1F015A5EDD83B72CCCEF56
SHA-256:	63EE732932BAEBE7BBF5E1214088CFDB908177FC3F6E9ECBF5DC9D12EC75A4F4
SHA-512:	E80E69328FA4C872FF33677DF6F29F5DF8A216C0272D42C5CB535DA787213A90D2B1334247E1D33D54A474D656E9990FBC07FC0C4ECFBEAADDFFCCBA00F082F7
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.=1.3.2.6.5.3.8.9.3.3.1.5.2.4.4.9.9.4.....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.=1.3.2.6.5.3.8.9.3.4.0.6.1.8.2.2.2.3.....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.=7.8.0.a.6.a.f.9.-.f.9.7.e.-.4.f.0.5.-.8.9.6.7.-.7.4.e.b.e.b.4.a.f.5.b.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=9.5.0.6.0.6.4.e.-.b.9.b.7.-.4.e.4.c.-.8.2.0.7.-.b.1.4.7.6.a.a.2.e.4.a.f.....W.o.w.6.4.H.o.s.t.=3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=3.3.2.....N.s.A.p.p.N.a.m.e.=r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=0.0.0.0.1.6.2.c.-.0.0.0.1.-.0.0.1.7.-.0.3.6.c.-.6.d.4.a.0.3.4.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=W.:0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.c.c.5.d.c.3.2.2.0.3.4.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\WER979A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini Dump crash report, 14 streams, Thu May 13 14:22:13 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	50834
Entropy (8bit):	2.100566131347861
Encrypted:	false
SSDEEP:	192:Xuk3ih9oEq161z3ypap1cGfzjuBwsbDa+mZfS2yrAnf74nM4O6:ek3i/JidpG12SADG5zyrA8PF
MD5:	7D52A7C222C360AA2FAD9CFB1DDD37B3
SHA1:	7E669387DEEE582EB153D8A80AA9EE1C19FC40ED
SHA-256:	935CACD80D6E239E08E15FCF3EE51C18545925FA6FCEE9E93BD2C296F1622460
SHA-512:	1FF225175FEF603D06409EBDEF451783E986A9828884186CEB273BAECA94904F6776A9EE1C8D89AC711D35ABE1E964D4314D3F3E25197EADA4D22E9DF642C0E5
Malicious:	false
Reputation:	low
Preview:	MDMP.....6.`.....U.....B.....GenuineIntelW.....T.....5.`.....0.=.....P.a.c.i.f.i.c..S.t.a.n.d.a.r.d..T.i.m.e.....P.a.c.i.f.i.c..D.a.y.l.i.g.h.t..T.i.m.e.....1.7.1.3.4..1...x.8.6.f.r.e...r.s.4..._r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,1.0...0..1.7.1.3.4..1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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):	3.6959129043694867
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNivs6R6YFP6xSgmfTVVS4zCpri89brnbsfu5m:RrlsNi06R6Yd6xSgmfTfSvrngfB
MD5:	3DDAD06210304D0E92905D2D9D587C1A
SHA1:	9FB4E5AC0B5C51565E213317549780925370C0C0
SHA-256:	167E9F3E0E9E5850AE3530661E1F546231D3EBC88A92A80925B2821AD0B884C7
SHA-512:	18DD673A63BF5F40149DFC934A3C373B0B7382BF04BAAB8CE370FD8C57CA9746022D7D24790E7332104ED665C1588A4C6B92FF7CD7686B3DA16087C94A3766E
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	
Reputation:	low
Preview:	..<?xml version="1.0" encoding="UTF-16"?>.....<WERReportMetadata>.....<OSVersionInformation>.....<Windows.NT.Version>1.0.0</Windows.NT.Version>.....<Build>1.7.1.3.4</Build>.....<Product>(0x3.0);. Windows. 1.0. .Pro. </Product>.....<Edition>Professional</Edition>.....<BuildString>1.7.1.3.4...1...amd64.free.rs4_.re.le.a.se...1.8.0.4.1.0.-1.8.0.4. </BuildString>.....<Revision>1</Revision>.....<Flavor>Multiprocessor.Free</Flavor>.....<Architecture>X64</Architecture>.....<LCID>1.0.3.3</LCID>.....</OSVersionInformation>.....<ProcessInformation>.....<Pid>5.6.7.6</Pid>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA95F.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):	4.473801425574143
Encrypted:	false
SSDEEP:	48:cvlwSD8zsHJgtWI9Y2WSC8Bb8fm8M4JCdsXnRFZ+q8/6NF44SrSYd:ulTfpDXSN+JtNPdNyDWYd
MD5:	BA2E0002234D1E42B5199B673F63273A
SHA1:	52688420F23A05AC86576DD4DE05A632D2400499
SHA-256:	C14DFD9137881C173A133A5DCB22C43089A8068ED71BA2F638C8ED1B7900D489
SHA-512:	8D2889E6301F3654D7092C5F7CD9146812E66553552EDDEE92DCFAF8B9D50DD0FBE3EF7D1197D55FC80FE4DD5241678E8773337654E1C2BEDDC6F5A9C82C2E2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="987812" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General	
File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
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
SHA256:	b5c92ef90ff138ee8edecb4250170ca12bd1e0b1fcdc58527121bea0f104b504
SHA512:	d8145cf3397f8eae35ed14c6f895dcf278e16b8a92c1d345325909225ce2c9dbcd08befe720f43d54c025858c999a0ec531603206616f710ecc6aec3dfeff6e3
SSDEEP:	3072:h9F/oNrQb4xVubbXP/NTccbsFvCeLmXH57V30e8Pj:h9F6QXvFczyYpQP
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:	74f0e4ecccde0e4

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

[illegible]

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

Description	Data
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 07:21:32.078113079 CEST	61242	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:32.138245106 CEST	53	61242	8.8.8.8	192.168.2.7
May 13, 2021 07:21:33.438667059 CEST	58562	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:33.487343073 CEST	53	58562	8.8.8.8	192.168.2.7
May 13, 2021 07:21:34.049644947 CEST	56590	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:34.106904984 CEST	53	56590	8.8.8.8	192.168.2.7
May 13, 2021 07:21:34.245975018 CEST	60501	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:34.294497967 CEST	53	60501	8.8.8.8	192.168.2.7
May 13, 2021 07:21:35.594439030 CEST	53775	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:35.643178940 CEST	53	53775	8.8.8.8	192.168.2.7
May 13, 2021 07:21:37.099231005 CEST	51837	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:37.161634922 CEST	53	51837	8.8.8.8	192.168.2.7
May 13, 2021 07:21:38.668080091 CEST	55411	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:38.716939926 CEST	53	55411	8.8.8.8	192.168.2.7
May 13, 2021 07:21:39.613085985 CEST	63668	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:39.661848068 CEST	53	63668	8.8.8.8	192.168.2.7
May 13, 2021 07:21:40.776583910 CEST	54640	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:40.828876972 CEST	53	54640	8.8.8.8	192.168.2.7
May 13, 2021 07:21:41.632611990 CEST	58739	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:41.684180975 CEST	53	58739	8.8.8.8	192.168.2.7
May 13, 2021 07:21:45.412739992 CEST	60338	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:45.461476088 CEST	53	60338	8.8.8.8	192.168.2.7
May 13, 2021 07:21:46.287682056 CEST	58717	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:46.346251011 CEST	53	58717	8.8.8.8	192.168.2.7
May 13, 2021 07:21:47.529454947 CEST	59762	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:47.578155994 CEST	53	59762	8.8.8.8	192.168.2.7
May 13, 2021 07:21:48.706271887 CEST	54329	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:48.755271912 CEST	53	54329	8.8.8.8	192.168.2.7
May 13, 2021 07:21:49.642894983 CEST	58052	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:49.694606066 CEST	53	58052	8.8.8.8	192.168.2.7
May 13, 2021 07:21:51.201767921 CEST	54008	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:51.250580072 CEST	53	54008	8.8.8.8	192.168.2.7
May 13, 2021 07:21:52.049643993 CEST	59451	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:52.098423958 CEST	53	59451	8.8.8.8	192.168.2.7
May 13, 2021 07:21:53.379245996 CEST	52914	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:53.436544895 CEST	53	52914	8.8.8.8	192.168.2.7
May 13, 2021 07:21:54.898844004 CEST	64569	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:54.958354950 CEST	53	64569	8.8.8.8	192.168.2.7
May 13, 2021 07:21:58.627784014 CEST	52816	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:58.684894085 CEST	53	52816	8.8.8.8	192.168.2.7
May 13, 2021 07:21:59.944164038 CEST	50781	53	192.168.2.7	8.8.8.8
May 13, 2021 07:21:59.995670080 CEST	53	50781	8.8.8.8	192.168.2.7
May 13, 2021 07:22:01.075503111 CEST	54230	53	192.168.2.7	8.8.8.8
May 13, 2021 07:22:01.124047995 CEST	53	54230	8.8.8.8	192.168.2.7
May 13, 2021 07:22:22.218527079 CEST	54911	53	192.168.2.7	8.8.8.8
May 13, 2021 07:22:22.276673079 CEST	53	54911	8.8.8.8	192.168.2.7
May 13, 2021 07:22:23.830853939 CEST	49958	53	192.168.2.7	8.8.8.8
May 13, 2021 07:22:23.895991087 CEST	53	49958	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2021 07:22:25.997685909 CEST	50860	53	192.168.2.7	8.8.8.8
May 13, 2021 07:22:26.055222034 CEST	53	50860	8.8.8.8	192.168.2.7
May 13, 2021 07:22:43.317138910 CEST	50452	53	192.168.2.7	8.8.8.8
May 13, 2021 07:22:43.374423981 CEST	53	50452	8.8.8.8	192.168.2.7
May 13, 2021 07:23:13.839014053 CEST	59730	53	192.168.2.7	8.8.8.8
May 13, 2021 07:23:13.887625933 CEST	53	59730	8.8.8.8	192.168.2.7
May 13, 2021 07:23:16.982786894 CEST	59310	53	192.168.2.7	8.8.8.8
May 13, 2021 07:23:17.050173044 CEST	53	59310	8.8.8.8	192.168.2.7
May 13, 2021 07:23:26.280596972 CEST	51919	53	192.168.2.7	8.8.8.8
May 13, 2021 07:23:26.339200974 CEST	53	51919	8.8.8.8	192.168.2.7
May 13, 2021 07:23:42.311078072 CEST	64296	53	192.168.2.7	8.8.8.8
May 13, 2021 07:23:42.368103981 CEST	53	64296	8.8.8.8	192.168.2.7
May 13, 2021 07:23:43.056982040 CEST	56680	53	192.168.2.7	8.8.8.8
May 13, 2021 07:23:43.116476059 CEST	53	56680	8.8.8.8	192.168.2.7
May 13, 2021 07:23:43.718794107 CEST	58820	53	192.168.2.7	8.8.8.8
May 13, 2021 07:23:43.770204067 CEST	53	58820	8.8.8.8	192.168.2.7
May 13, 2021 07:23:44.058391094 CEST	60983	53	192.168.2.7	8.8.8.8
May 13, 2021 07:23:44.123290062 CEST	53	60983	8.8.8.8	192.168.2.7
May 13, 2021 07:23:44.330984116 CEST	49247	53	192.168.2.7	8.8.8.8
May 13, 2021 07:23:44.379803896 CEST	53	49247	8.8.8.8	192.168.2.7
May 13, 2021 07:23:44.950918913 CEST	52286	53	192.168.2.7	8.8.8.8
May 13, 2021 07:23:45.007890940 CEST	53	52286	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



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



Click to jump to process

System Behavior

Analysis Process: loadll32.exe PID: 4584 Parent PID: 5708

General

Start time:	07:21:39
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:	0xd0000
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: 2172 Parent PID: 4584

General

Start time:	07:21:39
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:	0x870000
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: 5676 Parent PID: 2172

General

Start time:	07:21:40
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:	0x3e0000
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: 00000002.00000002.338342680.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6892 Parent PID: 5676

General

Start time:	07:22:09
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5676 -s 764
Imagebase:	0x380000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6D251717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER979A.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER979A.tmp.dmp	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEA95F.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEA95F.tmp.xml	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_1abacc56	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_1abacc56\Report.wer	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D24497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER979A.tmp	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEA95F.tmp	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER979A.tmp.dmp	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEA95F.tmp.xml	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEA96C.tmp.csv	success or wait	1	6D244BEF	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAD84.tmp.txt	success or wait	1	6D244BEF	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER979A.tmp.dmp	unknown	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	...r.u.n.d.l.l.3.2...e.x.e...	success or wait	51	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER979A.tmp.dmp	unknown	752	00 00 93 73 00 00 00 00 00 30 02 00 b8 55 02 00 73 40 de 10 92 25 00 00 bd 04 ef fe 00 00 01 00 00 00 0a 00 01 00 ee 42 00 00 0a 00 01 00 ee 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 fb fe 0f 00 01 00 00 00 ff ff 13 00 00 00 01 00 00 00 01 00 00 00 00 00 ff ff fe 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 32 02 00 00 00 00 00 a0 d1 02 00 00 00 00 38 4a 01 00 00 01 00 00 00 00 00 00 ff ff ff ff 00 00 00 4e d6 00 00 00 00 00 00 7a 4d 03 00 00 00 00 00 b0 93 02 00 00 00 00 00 ff ff ff 00 00 00 00 0a 02 22 00 00 00 00 00 40 ff 1f 00 00 00 00 00 54 04 22 00 00 00 00	...s...0...U..s@...%.....B.....B?.....#..... ..@A.....Zb.....p2..... 8J.....N.....zM" @.....T."....	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER979A.tmp.dmp	unknown	10850	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	...E.v.e.n.t.....F.i.l.e.....F.i.l.e... (...W.a.i.t.C.o.m.p.l.e.t. i.o.n.P.a.c.k.e.t.....I.o.C. o.m.p.l.e.t.i.o.n.....T.p.W. o.r.k.e.r.F.a.c.t.o.r.y..... I.R.T.i.m.e.r...(W.a.i.t.C. o.m.p.l.e.t.i.o.n.P.a.c.k.e.t.I.R.T.i.m	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER979A.tmp.dmp	unknown	108	03 00 00 00 c4 00 00 00 fc 06 00 00 04 00 00 00 88 15 00 00 cc 07 00 00 05 00 00 00 24 01 00 00 a8 33 00 00 06 00 00 00 a8 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 c8 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 60 1e 00 00 7a a8 00 00 15 00 00 00 ec 01 00 00 54 1d 00 00 16 00 00 00 98 00 00 00 40 1f 00 00	\$. ...3.....T.....8..... ...T.....`...z..... ..T.....@...	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	ff fe	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./A.r.c.h.i.t.e.c.t.u.r.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<.L.C.I.D.>.1.0.3.3.<./L.C.I.D.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 35 00 36 00 37 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.5.6.7.6.<./P.i.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<.I.m.a.g.e.N.a.m.e.>.r.u.n.d.I.I.3.2...e.x.e.<./I.m.a.g.e.N.a.m.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<.C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.0.0.0.0.0.0.0.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e.>.	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 33 00 35 00 31 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<.U.p.t.i.m.e.>.3.3.5.1.4.<./U.p.t.i.m.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	88	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 38 00 32 00 33 00 38 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.8.2.3.8.7.2.<./P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	72	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 31 00 32 00 37 00 38 00 31 00 35 00 36 00 38 00 30 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.1.2.7.8.1.5.6.8.0.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 39 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<.P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.2.6.9.9.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 32 00 30 00 30 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.2.0.0.9.6.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 32 00 30 00 30 00 39 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.9.2.2.0.0.9.6.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.1.8.4.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 38 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.3.0.8.7.2.<./Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.3.0.6.0.0.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.I.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 39 00 38 00 32 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e>.5.8.9.8.2.4.0.<./P.a.g.e.f.i.l.e.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 39 00 30 00 36 00 34 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.5.9.0.6.4.3.2.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 38 00 39 00 38 00 32 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.5.8.9.8.2.4.0.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./P.r.o.c.e.s.s.V.m.I.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<.P.i.d.>.2.1.7.2.<./P.i.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.0.0.0.0.0.0.0.<./C.m.d.L.i.n.e.S.i.g.n.a.t.u.r.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 33 00 38 00 34 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>.3.3.8.4.7.<./U.p.t.i.m.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<I.p.t.E.n.a.b.l.e.d>.0.<./I.p.t.E.n.a.b.l.e.d>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 35 00 32 00 31 00 32 00 39 00 37 00 39 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<.V.i.r.t.u.a.l.S.i.z.e.>.5.2.1.2.9.7.9.2.<./V.i.r.t.u.a.l.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 36 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.>.1.1.2.6.<./P.a.g.e.F.a.u.l.t.C.o.u.n.t.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 34 00 33 00 37 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.4.3.7.4.4.<./P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 30 00 36 00 38 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<.W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.3.7.0.6.8.8.0.<./W.o.r.k.i.n.g.S.e.t.S.i.z.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 33 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.3.3.2.1.6.<./Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 39 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.4.9.5.2.<./Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.a.g.e.f.i.l.e.U.s.a.g.e.>.2.3.6.3.3.9.2.<./P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 31 00 36 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.3.6.1.6.7.6.8.<./P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	5	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<.P.r.i.v.a.t.e.U.s.a.g.e.>.2.3.6.3.3.9.2.<./P.r.i.v.a.t.e.U.s.a.g.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	4	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	8	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	16	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	6	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	12	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<.P.a.r.a.m.e.t.e.r.1.>.1.0...0...1.7.1.3.4...2...0...2.5.6...4.8.<./P.a.r.a.m.e.t.e.r.1.>.	success or wait	6	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.S.y.s.t.e.m.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 67 00 75 00 71 00 65 00 68 00 6d 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.>.g.u.q.e.h.m., .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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 67 00 75 00 71 00 65 00 68 00 6d 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>.g.u.q.e.h.m.7,..1.<./S.y.s.t.e.m.P.r.o.d.u.c.t.N.a.m.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 38 00 38 00 38 00 34 00 36 00 37 00 30 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<.O.S.I.n.s.t.a.l.l.D.a.t.e>.1.5.8.8.8.4.6.7.0.4.<./O.S.I.n.s.t.a.l.l.D.a.t.e>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	6	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<F.l.a.g.s.>.0.0.0.0.0.0.0.0.<./F.l.a.g.s.>.	success or wait	3	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 32 00 32 00 3a 00 31 00 33 00 5a 00 22 00 3e 00	<.P.r.o.c.e.s.s.T.i.m.e.l.i.n.e.s. .B.a.s.e.T.i.m.e.= ".2.0. 2.1.-.0.5.-.1.3.T.1.4.:2.2:.. 1.3.Z.">.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 36 00 37 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 38 00 30 00 37 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 38 00 30 00 37 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 32 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64	<.P.r.o.c.e.s.s. .A.s.I.d.= ".3.3.9". .P.I.D.= ".5.6.7.6". .U.p.t.i.m.e.M.S.= ".2.8.0.7.8". .T.i.m.e.S.i.n.c.e.C.r.e.a.t.i.o.n.M.S.= ".2.8.0.7.8". .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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<.R.e.p.o.r.t.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	98	3c 00 47 00 75 00 69 00 64 00 3e 00 37 00 38 00 30 00 61 00 36 00 61 00 66 00 39 00 2d 00 66 00 39 00 37 00 65 00 2d 00 34 00 66 00 30 00 35 00 2d 00 38 00 39 00 36 00 37 00 2d 00 37 00 34 00 65 00 62 00 65 00 62 00 34 00 61 00 66 00 35 00 62 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<.G.u.i.d.>.7.8.0.a.6.a.f.9.-.f.9.7.e.-.4.f.0.5.-.8.9.6.7.-.7.4.e.b.e.b.4.a.f.5.b.8.<./G.u.i.d.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	2	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 31 00 2d 00 30 00 35 00 2d 00 31 00 33 00 54 00 31 00 34 00 3a 00 32 00 32 00 3a 00 31 00 33 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<.C.r.e.a.t.i.o.n.T.i.m.e.>.2.0.2.1.-.0.5.-.1.3.T.1.4.:2.2.:1.3.Z.<./C.r.e.a.t.i.o.n.T.i.m.e.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	2	09 00	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<./R.e.p.o.r.t.l.n.f.o.r.m.a.t.i.o.n.>.	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.tmp.WERInternalMetadata.xml	unknown	4	0d 00 0a 00		success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9FC9.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	6D24497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA95F.tmp.xml	unknown	4663	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>.. ver="2">.. <tlm>.. <src> .. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verblid" val="	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_1abacc56\Report.wer	unknown	2	ff fe	..	success or wait	1	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_1abacc56\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	6D24497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_rundll32.exe_63ae78cedc1f18d2762891f1bdcc4b2a36b2_82810a17_1abacc56\Report.wer	unknown	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 38 00 35 00 34 00 31 00 39 00 30 00 32 00 36 00 37 00	M.e.t.a.d.a.t.a.H.a.s.h.=.1. 8.5.4.1.9.0.2.6.7.	success or wait	1	6D24497A	unknown

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

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{\bfe0cd43-26bf-b938-53d2-233fa46f2f43}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{\bfe0cd43-26bf-b938-53d2-233fa46f2f43}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{\bfe0cd43-26bf-b938-53d2-233fa46f2f43}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	success or wait	1	6D2636BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6D261FB2	RegCreateKeyExW
\REGISTRY\A\{\bfe0cd43-26bf-b938-53d2-233fa46f2f43}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6D2443D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{\bfe0cd43-26bf-b938-53d2-233fa46f2f43}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	ProgramId	unicode	0000f519fec486de87ed73cb92d3cac802400000000	success or wait	1	6D2636BF	unknown
\REGISTRY\A\{\bfe0cd43-26bf-b938-53d2-233fa46f2f43}\Root\InventoryApplicationFile\rundll32.exe\ab97b57a	FileId	unicode	0000bcc5dc3222034d3f257f1fd35889e5be90f09b5f	success or wait	1	6D2636BF	unknown

