ID: 752975
Sample Name: pzG0rkIchr.exe
Cookbook: default.jbs
Time: 05:18:08
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

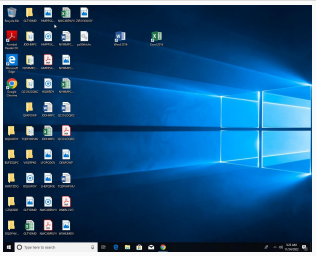
Windows Analysis Report

pzG0rkIchr.exe

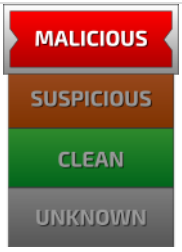
Overview

General Information

Sample Name:	pzG0rkIchr.exe (renamed file extension from exe to dll)
Analysis ID:	752975
MD5:	d6ef4778f7dc9c3..
SHA1:	5dad8394ef37d5..
SHA256:	54de1f2c26a63a..
Tags:	exe LDR4
Infos:	



Detection



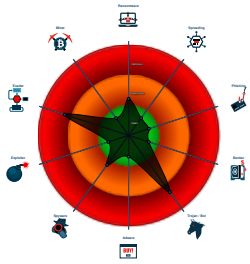
Ursnif

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Ursnif
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Performs DNS queries to domains w…
- One or more processes crash
- Contains functionality to check if a d…
- May sleep (evasive loops) to hinder…
- Internet Provider seen in connection…
- Detected potential crypto function
- Contains functionality to query CPU…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 492 cmdline: loaddll64.exe "C:\Users\user\Desktop\pzG0rkIchr.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 5284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5156 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pzG0rkIchr.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 1228 cmdline: rundll32.exe "C:\Users\user\Desktop\pzG0rkIchr.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 5172 cmdline: regsvr32.exe /s C:\Users\user\Desktop\pzG0rkIchr.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 400 cmdline: rundll32.exe C:\Users\user\Desktop\pzG0rkIchr.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2100 cmdline: rundll32.exe C:\Users\user\Desktop\pzG0rkIchr.dll,ItsnPq5v MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 5904 cmdline: C:\Windows\system32\WerFault.exe -u -p 2100 -s 304 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - WerFault.exe (PID: 5968 cmdline: C:\Windows\system32\WerFault.exe -u -p 2100 -s 304 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 1308 cmdline: rundll32.exe C:\Users\user\Desktop\pzG0rkIchr.dll,QlqYo259k MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 5188 cmdline: C:\Windows\system32\WerFault.exe -u -p 1308 -s 304 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - WerFault.exe (PID: 3260 cmdline: C:\Windows\system32\WerFault.exe -u -p 1308 -s 304 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "c2_domain": [
    "https://gigimas.xyz",
    "https://reaso.xyz"
  ],
  "botnet": "202206061",
  "aes key": "eq2opFFpGzpd2p9t",
  "sleep time": "20",
  "request time": "30",
  "host keep time": "120",
  "host shift time": "120"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: loaddll64.exe PID: 492	JoeSecurity_Ursnif v4	Yara detected Ursnif	Joe Security	
Process Memory Space: regsvr32.exe PID: 5172	JoeSecurity_Ursnif v4	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 1228	JoeSecurity_Ursnif v4	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 400	JoeSecurity_Ursnif v4	Yara detected Ursnif	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.48.8.8.864906532039645 11/24/22-05:22:35.810533
SID:	2039645
Source Port:	64906
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.48.8.8.861007532039645 11/24/22-05:20:02.978332
SID:	2039645
Source Port:	61007
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.48.8.8.861124532039645 11/24/22-05:21:04.451832
SID:	2039645
Source Port:	61124
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.48.8.8.859444532039645 11/24/22-05:21:34.871041
SID:	2039645
Source Port:	59444
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.48.8.8.855570532039645 11/24/22-05:22:05.359167
SID:	2039645
Source Port:	55570
Destination Port:	53

Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.860686532039645 11/24/22-05:20:33.386749
SID:	2039645
Source Port:	60686
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.859446532039645 11/24/22-05:23:06.390786
SID:	2039645
Source Port:	59446
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Performs DNS queries to domains with low reputation

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Ursnif

E-Banking Fraud

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

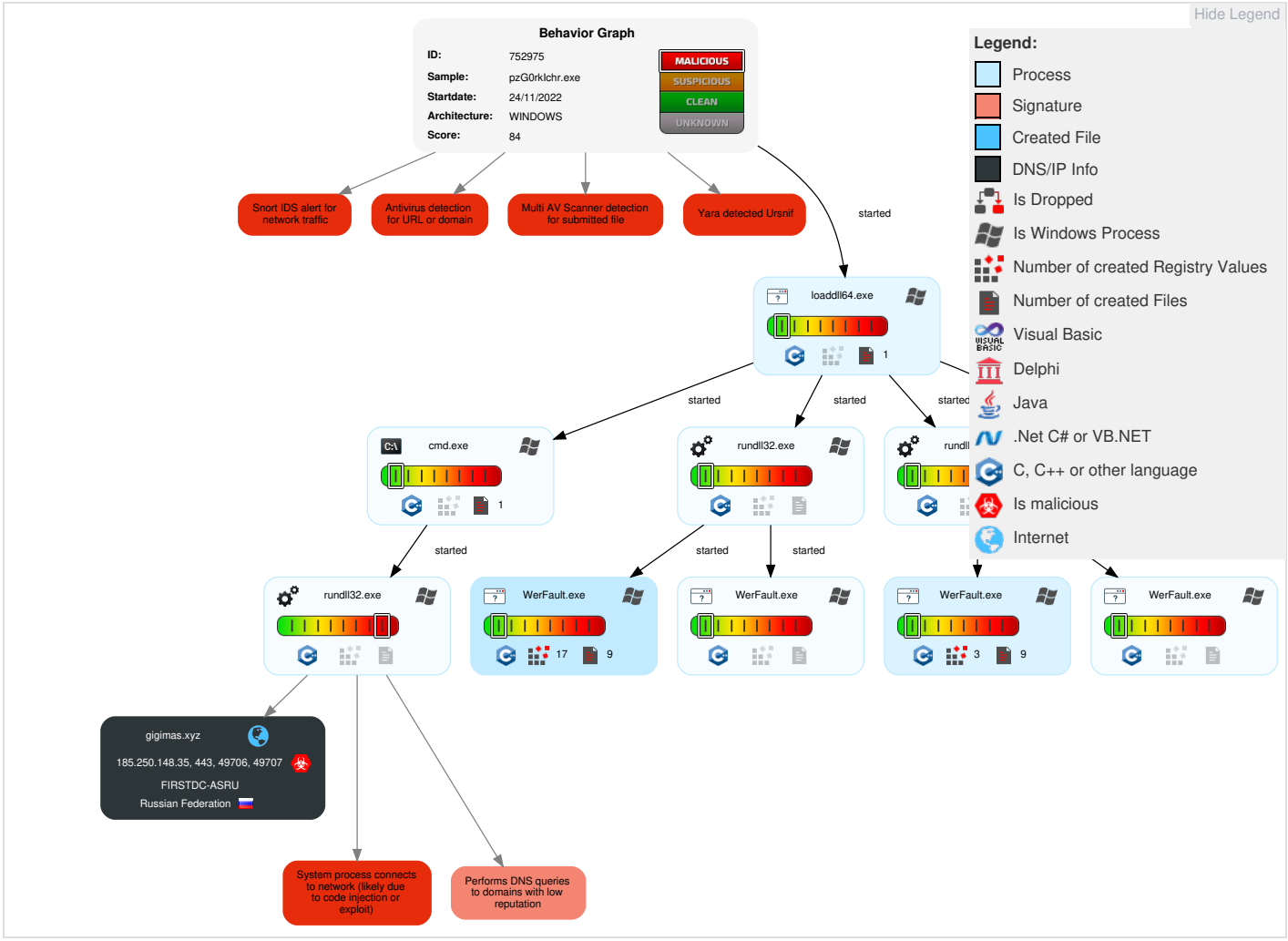
Yara detected Ursnif

Remote Access Functionality

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 1 2 Process Injection	1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 1 Virtualization/Sandbox Evasion	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 2 Process Injection	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Regsvr32	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

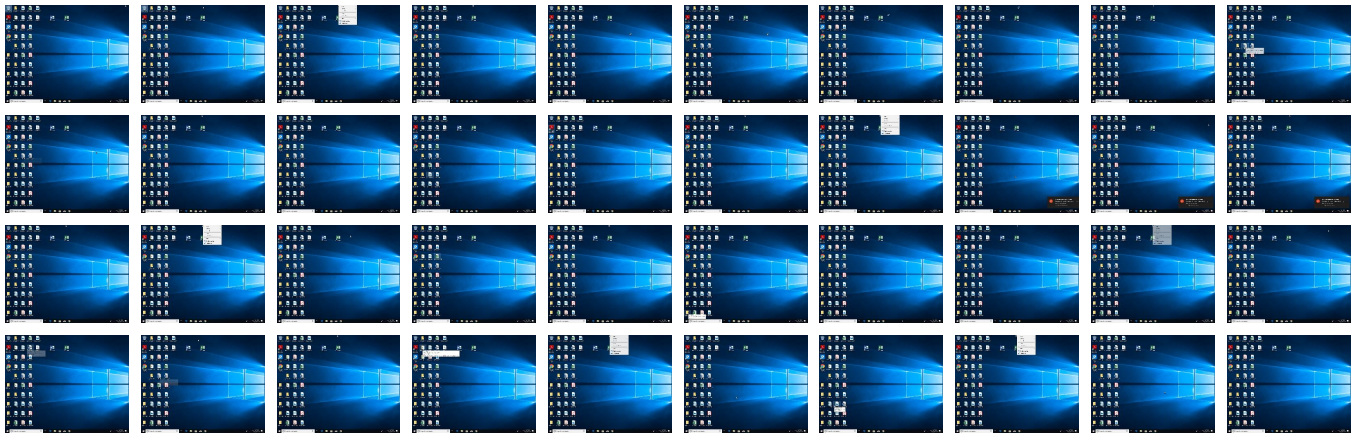
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
pzG0rklchr.dll	73%	ReversingLabs	Win64.Trojan.Tnega	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://gigimas.xyz/index.html)I6	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://https://gigimas.xyz/ic	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/index.htmlr	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/92	0%	Avira URL Cloud	safe	
http://https://Mozilla/5.0	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/index.htmll	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/index.htmluH	0%	Avira URL Cloud	safe	
http://https://gigimas.xyzhttps://reaso.xyz	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz:443/index.html	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/index.html	0%	Avira URL Cloud	safe	
http://https://reaso.xyz	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

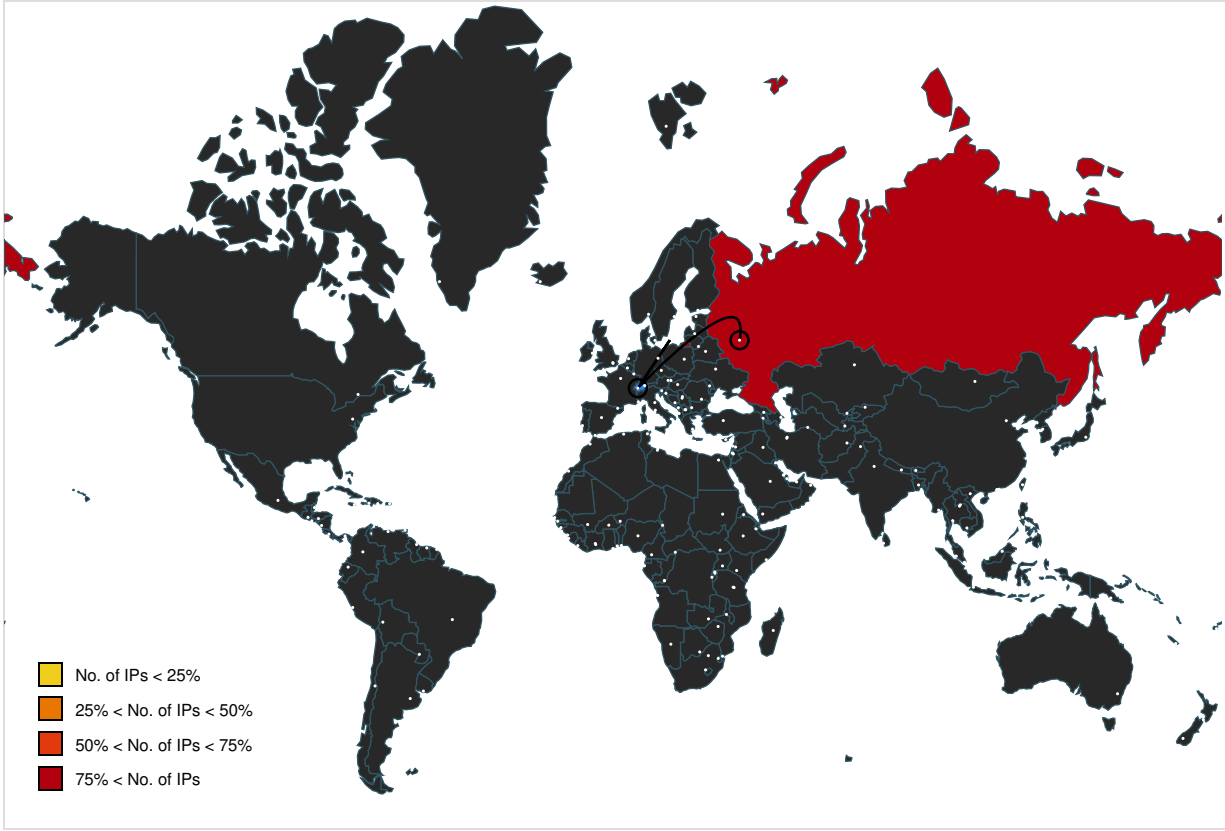
Name	IP	Active	Malicious	Antivirus Detection	Reputation
gigimas.xyz	185.250.148.35	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gigimas.xyz	loaddll64.exe, 00000000.00000003.4022719 14.0000027ED3940000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0003.00000003.388635168.0000000002100000 .00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000002.826743463.00000 21DDAD90000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000004.000 00002.826725063.0000021DDAC4D000.0000000 4.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000003.388322445.000001F71CC60 000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http://https://gigimas.xyz/index.html)I6	rundll32.exe, 00000004.00000003.75903961 9.0000021DD923C000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000003.759733313.0000021DD923C000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.694516726.000002 1DD923C000.00000004.00000020.00020000.00 000000.sdmp, rundll32.exe, 00000004.0000 0003.629091178.0000021DD923C000.00000004 .00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.693778417.0000021DD923C0 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http:// crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http:// crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl 0	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http://ocsp.sectigo.com0	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http://https://gigimas.xyz/92	rundll32.exe, 00000004.00000003.43226729 3.0000021DD9200000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gigimas.xyz/index.htmlr	rundll32.exe, 00000004.00000003.49730001 2.0000021DD9221000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000003.497398978.0000021DD9226000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://gigimas.xyz/ic	rundll32.exe, 00000004.00000002.82505038 7.0000021DD91F4000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://gigimas.xyz/index.htmluH	rundll32.exe, 00000004.00000003.43211334 1.0000021DD9221000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://Mozilla/5.0	loaddll64.exe, 00000000.00000003.4022777 27.0000027ED3942000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0003.00000003.388644042.0000000002102000 .00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000002.826756799.000002 1DDAD92000.00000004.00000020.00020000.0 0000000.sdmp, rundll32.exe, 00000005.000 00003.388329786.000001F71CC62000.0000000 4.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http:// crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http://https://gigimas.xyz/index.html	rundll32.exe, 00000004.00000003.56391364 3.0000021DD9221000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0 #	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http://https://gigimas.xyzhttps://reaso.xyz	rundll32.exe, 00000004.00000002.82672506 3.0000021DDAC4D000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7 c0#	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http://https://gigimas.xyz/index.htmll	rundll32.exe, 00000004.00000003.56391364 3.0000021DD9221000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://gigimas.xyz/	rundll32.exe, 00000004.00000002.82505038 7.0000021DD91F4000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000003.758857404.0000021DD9255000. 00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.758869560.000002 1DD925F000.00000004.00000020.00020000.00 000000.sdmp, rundll32.exe, 00000004.0000 0003.693664493.0000021DD925F000.00000004 .00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://reaso.xyz	rundll32.exe, 00000004.00000002.82672506 3.0000021DDAC4D000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 005.00000003.388322445.000001F71CC60000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://gigimas.xyz:443/index.html	rundll32.exe, 00000004.00000002.82503209 8.0000021DD91ED000.00000004.00000020.000 20000.00000000.sdmp, rundll32.exe, 00000 004.00000002.825050387.0000021DD91F4000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.250.148.35	gigimas.xyz	Russian Federation		48430	FIRSTDC-ASRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	752975
Start date and time:	2022-11-24 05:18:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pzG0rklchr.exe (renamed file extension from exe to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
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:	mal84.troj.evad.winDLL@22/8@7/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 68.3% (good quality ratio 59.4%) • Quality average: 56.9% • Quality standard deviation: 33.4%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.182.143.212
- Excluded domains from analysis (whitelisted): onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- VT rate limit hit for: pzG0rkIchr.dll

Simulations

Behavior and APIs

Time	Type	Description
05:19:48	API Interceptor	1x Sleep call for process: loaddll64.exe modified
05:19:49	API Interceptor	2x Sleep call for process: WerFault.exe modified
05:20:02	API Interceptor	6x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_5df03237c245e7792ae728ba7af47d1bed8c47f7_4f0e5919_16399239\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7600039551007107
Encrypted:	false

SSDEEP:	96:6TFZZFigJPnyqjs55P7HfipXIQcQHc6CcEm6cw3I/XaXz+HbHgSQgJPbpIDV9wO7:snigJKKH5Gs60j0I/u7swS274ltC
MD5:	BD5C8925F7120E1292DBD4961E9F2AB2
SHA1:	997623AC245EEC6535D175E199A180D43E9282FC
SHA-256:	0B242B11BC21F42FD27F1BDD633316DA3694606201E59C3C3CCC3593345C8B7A
SHA-512:	8075C625810E044C3224941D33DD97830E1EC5397E416AFC0DCCCB749580837F7629D7DDDCD531D39423195F82DCF2DF3060474F749789A977EF7DB655E6558
Malicious:	false
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.=.1.3.3.1.3.7.3.7.1.8.4.9.4.9.5.4.2.3.....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.=.1.3.3.1.3.7.3.7.1.8.6.9.4.9.5.2.0.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.e.8.6.8.a.2.1.-.d.3.3.a.-.4.6.6.6.-.b.2.e.f.-.6.8.2.8.6.b.5.0.0.f.9.5.....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.=.a.d.0.2.5.9.3.b.-.0.7.1.f.-.4.6.8.2.-.a.3.3.f.-.9.f.6.a.a.8.a.a.a.e.8.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.p.z.G.0.r.k.l.c.h.r...d.l.l.....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.=.0.0.0.0.0.8.3.4.-.0.0.0.1.-.0.0.1.f.-.3.5.4.2.-.0.2.e.4.b.b.f.f.d.8.0.1.....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.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_f6b0ff3966a3d6c74191edf638977ebb42334d7_4f0e5919_156d919c\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7599992295897045
Encrypted:	false
SSDEEP:	96:icFXVFiXJPnybjs55P7Hf5pXIQcQdc6/RcEccw3+XaXz+HbHgSQgJPbpIDV9wOyk:71iXJKlHz9mAj0I/u7swS274ltC
MD5:	1E8445DB848C561B6CB8CBEF60359786
SHA1:	00E829DA03ACB0B24004E2C2E45E7D439352BF8D
SHA-256:	8F94F06BC63F693379833D7156EC4C3E65788BD94BC7470C12EF985AED723EBD
SHA-512:	72C3DE3F22801E3947FDC86690B8A63175DC9EFCF7503AF898485A380B6941C42E55F965658B3F799051283C10C4823F5C0C2DE8EFE293C9904D117487FDA1D2
Malicious:	false
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.=.1.3.3.1.3.7.3.7.1.8.5.0.8.6.8.0.1.2.....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.=.1.3.3.1.3.7.3.7.1.8.7.2.8.9.9.3.1.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.b.1.b.0.7.4.e.-.3.1.b.5.-.4.4.2.6.-.9.9.a.5.-.9.9.5.d.d.3.d.8.4.c.8.4.....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.=.e.2.5.1.b.f.8.e.-.f.c.a.f.-.4.9.c.0.-.9.1.b.f.-.f.7.b.f.3.9.f.f.a.0.f.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.p.z.G.0.r.k.l.c.h.r...d.l.l.....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.=.0.0.0.0.0.5.1.c.-.0.0.0.1.-.0.0.1.f.-.8.9.9.5.-.c.1.e.6.b.b.f.f.d.8.0.1.....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.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Nov 24 04:19:45 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	56070
Entropy (8bit):	1.7075050210528775
Encrypted:	false
SSDEEP:	192:rlRq3OC5I6Pdfek5ka0LGuO3bcmXJBjz2RdYnUQDfERORDNKyB4RSOnR:pCDck5DbRD
MD5:	1A5AA058B4E8ACA002D6B153E7C3B88E
SHA1:	B722FD3B879CCAD5D57716D5D375355C05AC1AA4
SHA-256:	4C914A886A7765E4A814BD13405293A39423A4BB8A6EE712B7D48B0E3086A3F9
SHA-512:	010E25A468C02F293CEBCAF7FA64CF746F6716571837CAD3BC35877EC74F8808B352E2DBC3CE080FF502E1CE8ED8EF02F69F4953C48FFC0537CC6363A68EA7 2
Malicious:	false
Preview:	MDMP..... .....~c.....)..... T.....8..... T.....&..... T.....@.....U.....B.....Lw..... .....,nq...T.....4.....~c.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...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..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Nov 24 04:19:46 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	54966
Entropy (8bit):	1.7301605700636602
Encrypted:	false
SSDEEP:	192:kl9crsOC5We/Q7NLbBjD4z5s0mE6liAU3Oq:amC8e/Q7d1V0m
MD5:	A57C13F28721473003BE444D7239D372

SHA1:	10C6496461E1C6113B6FF62120CA7D83CC17216A
SHA-256:	EBF7FC039C185490580CF4BB3044B63044A13DD5305F7755AC858779DDFCD9FA
SHA-512:	814B8BD3E2333F3084A46553787236EE0C5C0B71EA62B6636836254D80939B593CC3AE58EABC8CD3DDAE9620CAC53AF5550504734A192F8BADBE8BA98EEA58 2A
Malicious:	false
Preview:	MDMP....... ....~c...)..........T.......8...........T...........................T...........@...U...........B.............Lw................ ....T............~c.............................0.................W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.......................................W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e................................ ......1.7.1.3.4...1...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... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8526
Entropy (8bit):	3.696693878810589
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWpWiN6Y+TagmfQYSl2G+prD89b4oCafaIm:RrlsNiYWiN6YKagmfQYSlR4FafE
MD5:	891C13F961FC9780F58F08B88D03FE00
SHA1:	7AC38531C1F3F85ED591B419A1C0C9D560DE4B1B
SHA-256:	B04D603146FD1D2F17D6588066AA48A86D85B511E7D88380393C69F9BCC4575C
SHA-512:	3D766FCF4F2835FD6750E5BED7331A27EF548BB8C9D729E7B3D3AD8AA09677360AE67F5F2887B1D8057FEBFC622505A4A179A2F07B31E87FBDCEFD4B42C2B4 77
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.......<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.........<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.........<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.........<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.........<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.........<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.........<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.........<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.........<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.........<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.......<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.......<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.........<.P.i.d.>.2.1.0. 0.<./.P.i.d.>.......

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8524
Entropy (8bit):	3.6955697518324317
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNivSLis6Y+ZagmfQhSGG+pr889b4IOfxIm:RrlsNiqLis6YgagmfQhSM4Zfr
MD5:	64CB5AA88613858B4078E5BB14479AE6
SHA1:	138C49AF256A227F26D86557778AADF52F016EFB
SHA-256:	1001101306104ACE07059DB78333327804781A7FBC4E59CBC7DEB3AC14A27E8E
SHA-512:	32B368E68F5C667FE75F2B36BECB8680A2D39960E69878D527CAC83B1356126C7BFA04C9645E17A0ACCC7482F244DC7A5571186F0B5F7371D39FF7579A2F5F6
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.......<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.........<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.........<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.........<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.........<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.........<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.........<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.........<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.........<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.........<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.......<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.......<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.........<.P.i.d.>.1.3.0. 8.<./.P.i.d.>.......

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8589.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4733
Entropy (8bit):	4.474599386008591
Encrypted:	false
SSDEEP:	48:cvIwSD8zsA+JgtBI9XlVWgc8sqYjRTq8fm8M4JCXCOFFVyq85m27UZESC5S+d:uITf3NGgrsqYlTfJ8xVv+d
MD5:	CDE8A3EB67D3F603A55F6BCA1C15EA67
SHA1:	9425363A7B60C24BB7466FEAA6C38D60B86C084D
SHA-256:	F2E7CAB0595409E2A61035A46D0DF145C3CCCDC99C2FE8FDB7BBF04B590ED7F9

SHA-512:	BC28D09B0C638843187EDB12E207B49C15A1F99917950FC5E748FEC26F62376E8AFDA47C3BBBEDB80F52FC38BF4C8FE02AA0232816274B4B291A576CD030FAC
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1793610" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER8683.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4733
Entropy (8bit):	4.478085829501657
Encrypted:	false
SSDEEP:	48:cvIwSD8zsA+JgtBI9XlVWgc8sqYjF8fm8M4JCXCOCFUyq85m2skUZESC5Sjd:uITf3NGgrsqYeJuzTVvjd
MD5:	0BD2A0E70F01F1D342661314591029DC
SHA1:	CFA327EBD0E02AEAA2F23AB3EA938AA843FB71F5
SHA-256:	A8350E49452A0A6A302EF0A3BA63447E4F1C64FF6C2335E22D1B53DE654A27D5
SHA-512:	6CA8CB1FA55453B637117B22CC0C474110CFE03BCFD602657AEE4F778B4072F8623D5CF32193183DF148F8A5630996B0926C499700F663552898C875774CD12A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1793610" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.637392883592079
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	pzG0rkIchr.dll
File size:	290568
MD5:	d6ef4778f7dc9c31a0a2a989ef42d2fd
SHA1:	5dad8394ef37d5a006674589754f7a3187d303b1
SHA256:	54de1f2c26a63a8f6b7f8d5de99f8ebd4093959ab07f027db1985d0652258736
SHA512:	997b57424364ff661d80ca6efc5b7e91f2204d1ed7c4d784ee7d6134bc06952c993de038d6a25c71a7949b08ddd8cc5d167f8c753379f69ee1b6b49342fafa63
SSDEEP:	6144:wHyvumb1p7CC8VoxOJbceNOHI2Tse2RTggR/Znv+yit:Smbrgu2so2TVwcK/ZnG/t
TLSH:	ED54BF41F3D904A6D9138D3D8857562BEBF13C212214DA5F8B50C36A6F37BA1E739B22
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!5..eT..eT..eT....Z.`T....X..T....Y.hT..^...bT..^...qT..^...uT....`.fT..eT...T.....gT.....dT.....dT..RicheT.....PE..d..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18000b6ec
Entrypoint Section:	.text

Digitally signed:	true
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x62C42DD7 [Tue Jul 5 12:25:59 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	4270d9bbb54b179372d82277269282e6

Authenticode Signature	
Signature Valid:	**true**
Signature Issuer:	CN=Sectigo Public Code Signing CA R36, O=Sectigo Limited, C=GB
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 7/6/2021 2:00:00 AM 7/7/2022 1:59:59 AM
Subject Chain	• CN=NAILS UNLIMITED LIMITED, O=NAILS UNLIMITED LIMITED, L=DORCHESTER, S=Dorset, C=GB
Version:	3
Thumbprint MD5:	71834A68FD130C9D08796B4F19A6FC67
Thumbprint SHA-1:	CA69087AAAA087346202AD16228337130511C4C5
Thumbprint SHA-256:	F13E4801E13898E839183E3305E1DDA7F4C0EBF6EAF7553E18C1DDD4EDC94470
Serial:	2F96A89BFEC6E44DD224E8FD7E72D9BB

Entrypoint Preview
Instruction
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007FE818B824F7h
call 00007FE818B828F0h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007FE818B8236Ch
int3

Instruction
int3
int3
dec eax
sub esp, 28h
call 00007FE818B82D88h
test eax, eax
je 00007FE818B82513h
dec eax
mov eax, dword ptr [00000030h]
dec eax
mov ecx, dword ptr [eax+08h]
jmp 00007FE818B824F7h
dec eax
cmp ecx, eax
je 00007FE818B82506h
xor eax, eax
dec eax
cmpxchg dword ptr [00038A68h], ecx
jne 00007FE818B824E0h
xor al, al
dec eax
add esp, 28h
ret
mov al, 01h
jmp 00007FE818B824E9h
int3
int3
int3
dec eax
sub esp, 28h
call 00007FE818B82D4Ch
test eax, eax
je 00007FE818B824F9h
call 00007FE818B82B6Fh
jmp 00007FE818B8250Bh
call 00007FE818B82D34h
mov ecx, eax
call 00007FE818B844A1h
test eax, eax
je 00007FE818B824F6h
xor al, al
jmp 00007FE818B824F9h
call 00007FE818B84828h
mov al, 01h
dec eax
add esp, 28h
ret
dec eax
sub esp, 28h
xor ecx, ecx
call 00007FE818B82636h
test al, al
setne al
dec eax
add esp, 28h
ret
int3
int3

Rich Headers

Programming Language:	• [C++] VS2015 UPD3.1 build 24215 • [EXP] VS2015 UPD3.1 build 24215 • [LNK] VS2015 UPD3.1 build 24215

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x371c0	0x94	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x37254	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x46000	0x15cc	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x44600	0x2908	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x49000	0x618	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x34dd0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x34df0	0x94	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x23000	0x2a8	.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	0x21390	0x21400	False	0.6091694078947368	zlib compressed data	6.321988758719223	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x23000	0x14b40	0x14c00	False	0.5551228350903614	data	5.589680054404924	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0xd378	0xc200	False	0.581286243556701	data	4.475772855701728	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x46000	0x15cc	0x1600	False	0.49556107954545453	data	5.3249872988992655	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gfids	0x48000	0x94	0x200	False	0.248046875	data	1.4095612964443904	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x49000	0x618	0x800	False	0.54150390625	data	4.760086879502757	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	CreateFileA, LockFile, ReadFile, SetEndOfFile, UnlockFile, CloseHandle, PeekNamedPipe, HeapCreate, HeapAlloc, HeapFree, GetProcessHeap, HeapWalk, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, TryEnterCriticalSection, DeleteCriticalSection, WaitForSingleObject, ExitProcess, CreateThread, VirtualAlloc, GetProcAddress, CreateFileMappingA, LoadLibraryA, CreateNamedPipeA, CallNamedPipeA, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, IsProcessorFeaturePresent, GetModuleHandleW, RtlUnwindEx, InterlockedFlushSList, GetLastError, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, GetCurrentProcess, TerminateProcess, GetModuleHandleExW, GetModuleFileNameA, MultiByteToWideChar, WideCharToMultiByte, LCMapStringW, FindClose, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, GetStdHandle, GetFileType, GetStringTypeW, CreateFileW, HeapSize, HeapReAlloc, SetStdHandle, FlushFileBuffers, WriteFile, GetConsoleCP, GetConsoleMode, ReadConsoleW, SetFilePointerEx, WriteConsoleW, RaiseException

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180002380

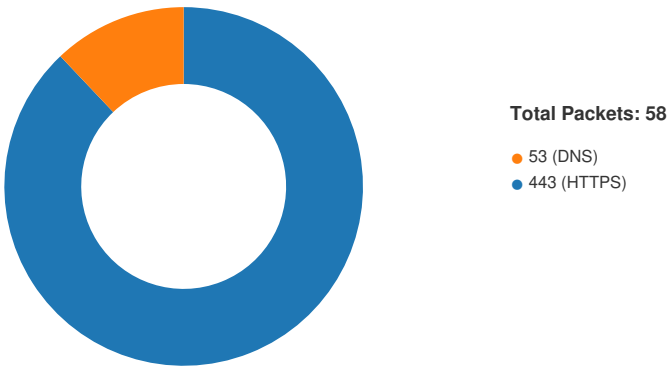
Name	Ordinal	Address
ItsnPq5v	2	0x180002390
QlqYo259k	3	0x180017c20
XeFnYZ409	4	0x1800175e0

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.48.8.8.8649065 32039645 11/24/22-05:22:35.810533	UDP	2039645	ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz)	64906	53	192.168.2.4	8.8.8.8
192.168.2.48.8.8.8610075 32039645 11/24/22-05:20:02.978332	UDP	2039645	ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz)	61007	53	192.168.2.4	8.8.8.8
192.168.2.48.8.8.8611245 32039645 11/24/22-05:21:04.451832	UDP	2039645	ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz)	61124	53	192.168.2.4	8.8.8.8
192.168.2.48.8.8.8594445 32039645 11/24/22-05:21:34.871041	UDP	2039645	ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz)	59444	53	192.168.2.4	8.8.8.8
192.168.2.48.8.8.8555705 32039645 11/24/22-05:22:05.359167	UDP	2039645	ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz)	55570	53	192.168.2.4	8.8.8.8
192.168.2.48.8.8.8606865 32039645 11/24/22-05:20:33.386749	UDP	2039645	ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz)	60686	53	192.168.2.4	8.8.8.8
192.168.2.48.8.8.8594465 32039645 11/24/22-05:23:06.390786	UDP	2039645	ET TROJAN Observed DNS Query to Ursnif Domain (gigimas .xyz)	59446	53	192.168.2.4	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 05:20:03.012599945 CET	49706	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.012650967 CET	443	49706	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.012737036 CET	49706	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.016460896 CET	49706	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.016508102 CET	443	49706	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.072525024 CET	443	49706	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.074080944 CET	49707	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.074155092 CET	443	49707	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.074337959 CET	49707	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.075628996 CET	49707	443	192.168.2.4	185.250.148.35

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 05:20:03.075655937 CET	443	49707	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.131845951 CET	443	49707	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.133225918 CET	49708	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.133289099 CET	443	49708	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.133398056 CET	49708	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.134278059 CET	49708	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.134324074 CET	443	49708	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.191957951 CET	443	49708	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.193757057 CET	49709	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.193816900 CET	443	49709	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.193898916 CET	49709	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.194484949 CET	49709	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:03.194506884 CET	443	49709	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:03.250332117 CET	443	49709	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.407180071 CET	49710	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.407258034 CET	443	49710	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.407423019 CET	49710	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.408660889 CET	49710	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.408710957 CET	443	49710	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.463525057 CET	443	49710	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.465197086 CET	49711	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.465265036 CET	443	49711	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.465380907 CET	49711	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.466645002 CET	49711	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.466680050 CET	443	49711	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.522078991 CET	443	49711	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.525345087 CET	49712	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.525413036 CET	443	49712	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.525672913 CET	49712	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.526755095 CET	49712	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.526801109 CET	443	49712	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.582118988 CET	443	49712	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.585807085 CET	49713	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.585897923 CET	443	49713	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.586055040 CET	49713	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.586787939 CET	49713	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:20:33.586810112 CET	443	49713	185.250.148.35	192.168.2.4
Nov 24, 2022 05:20:33.641958952 CET	443	49713	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.485233068 CET	49714	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.485310078 CET	443	49714	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.485480070 CET	49714	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.486561060 CET	49714	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.486601114 CET	443	49714	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.541218996 CET	443	49714	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.542530060 CET	49715	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.542584896 CET	443	49715	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.542787075 CET	49715	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.543291092 CET	49715	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.543320894 CET	443	49715	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.598916054 CET	443	49715	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.600245953 CET	49716	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.600316048 CET	443	49716	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.600423098 CET	49716	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.600950003 CET	49716	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.600979090 CET	443	49716	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.668997049 CET	443	49716	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.685195923 CET	49717	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.685261965 CET	443	49717	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.685632944 CET	49717	443	192.168.2.4	185.250.148.35

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 05:21:04.686243057 CET	49717	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:04.686269045 CET	443	49717	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:04.742952108 CET	443	49717	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:34.890145063 CET	49718	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:34.890221119 CET	443	49718	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:34.890311956 CET	49718	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:34.891124010 CET	49718	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:34.891169071 CET	443	49718	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:34.949980021 CET	443	49718	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:34.951565027 CET	49719	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:34.951642990 CET	443	49719	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:34.951733112 CET	49719	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:34.952301979 CET	49719	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:34.952337027 CET	443	49719	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:35.007440090 CET	443	49719	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:35.008912086 CET	49720	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:35.008971930 CET	443	49720	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:35.009077072 CET	49720	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:35.009592056 CET	49720	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:35.009608984 CET	443	49720	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:35.066533089 CET	443	49720	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:35.083612919 CET	49721	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:35.083692074 CET	443	49721	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:35.083832026 CET	49721	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:35.084454060 CET	49721	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:21:35.084505081 CET	443	49721	185.250.148.35	192.168.2.4
Nov 24, 2022 05:21:35.141772032 CET	443	49721	185.250.148.35	192.168.2.4
Nov 24, 2022 05:22:05.380898952 CET	49722	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:22:05.380964041 CET	443	49722	185.250.148.35	192.168.2.4
Nov 24, 2022 05:22:05.381064892 CET	49722	443	192.168.2.4	185.250.148.35
Nov 24, 2022 05:22:05.382277966 CET	49722	443	192.168.2.4	185.250.148.35

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 05:20:02.978332043 CET	61007	53	192.168.2.4	8.8.8.8
Nov 24, 2022 05:20:02.997380018 CET	53	61007	8.8.8.8	192.168.2.4
Nov 24, 2022 05:20:33.386749029 CET	60686	53	192.168.2.4	8.8.8.8
Nov 24, 2022 05:20:33.404028893 CET	53	60686	8.8.8.8	192.168.2.4
Nov 24, 2022 05:21:04.451832056 CET	61124	53	192.168.2.4	8.8.8.8
Nov 24, 2022 05:21:04.469230890 CET	53	61124	8.8.8.8	192.168.2.4
Nov 24, 2022 05:21:34.871041059 CET	59444	53	192.168.2.4	8.8.8.8
Nov 24, 2022 05:21:34.888430119 CET	53	59444	8.8.8.8	192.168.2.4
Nov 24, 2022 05:22:05.359167099 CET	55570	53	192.168.2.4	8.8.8.8
Nov 24, 2022 05:22:05.377713919 CET	53	55570	8.8.8.8	192.168.2.4
Nov 24, 2022 05:22:35.810533047 CET	64906	53	192.168.2.4	8.8.8.8
Nov 24, 2022 05:22:35.829649925 CET	53	64906	8.8.8.8	192.168.2.4
Nov 24, 2022 05:23:06.390785933 CET	59446	53	192.168.2.4	8.8.8.8
Nov 24, 2022 05:23:06.408032894 CET	53	59446	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 05:20:02.978332043 CET	192.168.2.4	8.8.8.8	0x362c	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:20:33.386749029 CET	192.168.2.4	8.8.8.8	0x306e	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:21:04.451832056 CET	192.168.2.4	8.8.8.8	0xfd4e	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false

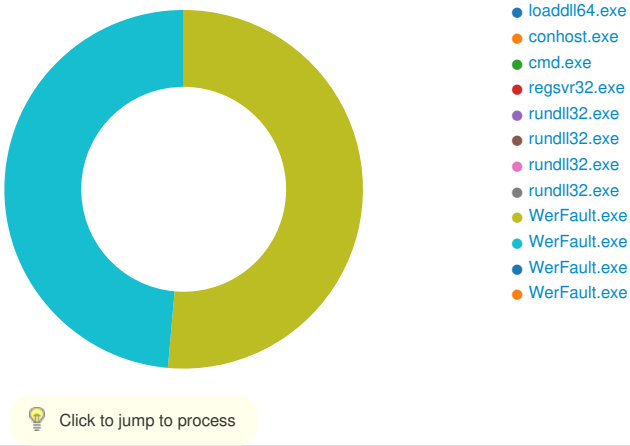
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 05:21:34.871041059 CET	192.168.2.4	8.8.8.8	0xbb49	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:22:05.359167099 CET	192.168.2.4	8.8.8.8	0xe9a0	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:22:35.810533047 CET	192.168.2.4	8.8.8.8	0x374b	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:23:06.390785933 CET	192.168.2.4	8.8.8.8	0x8724	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 24, 2022 05:20:02.997380018 CET	8.8.8.8	192.168.2.4	0x362c	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:20:33.404028893 CET	8.8.8.8	192.168.2.4	0x306e	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:21:04.469230890 CET	8.8.8.8	192.168.2.4	0xfd4e	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:21:34.888430119 CET	8.8.8.8	192.168.2.4	0xbb49	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:22:05.377713919 CET	8.8.8.8	192.168.2.4	0xe9a0	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:22:35.829649925 CET	8.8.8.8	192.168.2.4	0x374b	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:23:06.408032894 CET	8.8.8.8	192.168.2.4	0x8724	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 492, Parent PID: 3528

General

Target ID:	0
Start time:	05:19:01
Start date:	24/11/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\pzG0rkIchr.dll"
Imagebase:	0x7ff72b830000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5284, Parent PID: 492

General

Target ID:	1
Start time:	05:19:02
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5156, Parent PID: 492

General

Target ID:	2
Start time:	05:19:02
Start date:	24/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pzG0rkIchr.dll",#1
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5172**, Parent PID: **492**

General	
Target ID:	3
Start time:	05:19:02
Start date:	24/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\pzG0rkIchr.dll
Imagebase:	0x7ff762150000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **1228**, Parent PID: **5156**

General	
Target ID:	4
Start time:	05:19:02
Start date:	24/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\pzG0rkIchr.dll",#1
Imagebase:	0x7ff736ed0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **400**, Parent PID: **492**

General	
Target ID:	5
Start time:	05:19:02
Start date:	24/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\pzG0rkIchr.dll,DllRegisterServer
Imagebase:	0x7ff736ed0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **2100**, Parent PID: **492**

General	
Target ID:	6
Start time:	05:19:07
Start date:	24/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\pzG0rkIchr.dll,ItsnPq5v
Imagebase:	0x7ff736ed0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: **1308**, Parent PID: **492**

General	
Target ID:	9
Start time:	05:19:12
Start date:	24/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\pzG0rkIchr.dll,QlqYo259k
Imagebase:	0x7ff736ed0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **5904**, Parent PID: **2100**

General	
Target ID:	11
Start time:	05:19:18
Start date:	24/11/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 2100 -s 304
Imagebase:	0x7ff69db50000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF88B85527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8589.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8589.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_5df03237c245e7792ae728ba7af47d1bed8c47f7_4f0e5919_16399239	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_5df03237c245e7792ae728ba7af47d1bed8c47f7_4f0e5919_16399239\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8589.tmp	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8589.tmp.xml	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREBA.tmp.csv	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1081.tmp.txt	success or wait	1	7FF88B84E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7e 63 fd 05 12 00 00 00 00 00	MDMP ~c	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	5080	6	00 00 00 00 00 00		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	200	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 2c 6e 71 01 00 00 54 05 00 00 fd 03 00 00 34 08 00 00 fd fd 7e 63 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBLw,nqT4~c0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	5750	1232	60 77 49 3d fd 01 00 00 60 77 49 3d fd 01 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 fd 7f 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 06 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 55 48 3d fd 37 00 00 00 00 00 00 fd 52 48 3d fd 01 00 00 fd 01 00 00 00 00 00 00 50 fd fd 79 40 00 00 00 fd 37 00 00 00 00 00 00 fd 0b fd 36 00 00 00 00 fd 52 48 3d fd 01 00 00 fd 31 00 00 00 00 00 00 2c 1f 00 00 00 00 00 00 72 fd 11 fd 0f 00 00 08 fd fd 79 40 00 00 00 fd 31 00 00 00 00 00 00 fd 06 00 00 00 00 00 00 07 fd fd fd 00 00 00 00 49 12 fd 36 00 00 00 00 fd 07 fd fd 7f 00	\`wI=\`wI=_3++S++UH=7RH=Py@76RH=1,ry@1I6	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	1620	168	1c 14 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 07 fd fd 7f 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 76 16 00 00	v	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	10678	20	10 00 00 00 62 fd 07 fd fd 7f 00 00 00 01 00 00 fd 2a 00 00	b*	success or wait	16	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	10938	256	42 fd 44 3b 1d 66 03 00 74 fd fd 0b 48 63 0b fd 20 fd 43 04 fd fd 08 48 fd 49 fd 14 fd 0f fd fd 48 fd 0a 48 0f fd fd 48 fd 0a fd 4b 04 48 63 4b 04 48 fd 05 0d fd 03 00 48 fd fd 24 fd 00 00 00 0f fd 04 01 48 fd fd 60 41 5f 41 5e 41 5d 41 5c 5f 5e 5d fd fd fd fd fd fd fd fd fd fd 48 fd 5c 24 10 48 fd 6c 24 18 57 48 fd fd 20 48 fd fd fd 01 00 00 48 fd fd fd fd 58 01 00 00 48 fd fd 44 fd fd fd 00 00 00 41 fd fd 27 00 00 41 3b fd 75 12 33 fd 48 fd 5c 24 38 48 fd 6c 24 40 48 fd fd 20 5f fd 48 fd fd fd 00 00 00 48 35 fd 25 00 00 48 fd 74 24 30 48 09 fd fd 01 00 00 33 fd fd 15 28 fd 01 00 48 fd fd 74 40 4c fd fd 33 fd 48 fd fd fd 15 05 fd 01 00 48 fd fd fd 01 00 00 4c fd fd 48 fd fd fd fd 00 02 00 00 48 fd 01 fd fd 37 00 00 fd fd 28 00 00 48 fd 17 48 fd	BD;tHc CHIHHHKHcKHH$H`A_A ^A]A_^]H\$Hl$WH HHXHDA'A;u3H\$8Hl$ @H _HH5%Ht$0H3(Ht@L3H HLHH7(HH	success or wait	15	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	49074	1832	76 fd fd fd fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 fd fd fd 7f 00 00 10 00 00 00 00 00 00 00 18 fd fd 79 40 00 00 00 11 fd fd 79 40 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 20 fd 79 40 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 52 48 3d fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2f 48 3d fd 01 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	v`2y@y@ y@RH=/H=PP	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	1788	4	03 00 00 00		success or wait	3	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	6982	1232	00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd 6f 58 fd fd 7f 00 00 fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 78 fd fd 79 40 00 00 00 fd fd fd fd fd fd fd 78 fd fd 79 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 68 fd fd 79 40 00 00 00 fd fd fd 79 40 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 78 fd fd 79 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bf fd fd 7f 00	oX 3++S++Fxy@xy@hy@y @xy@	success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	1888	48	04 06 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 fd 79 40 00 00 00 fd fd fd 79 40 00 00 00 28 07 00 00 fd fd 00 00 fd 04 00 00 fd 24 00 00	py@y@($	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	1948	4	17 00 00 00		success or wait	23	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	5086	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	rundll32.exe	success or wait	23	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	4328	752	00 00 60 fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 5c 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 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 00 60 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 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 40 fd 02 00 00 00 00 00 fd 15 03 00 00 00 00 fd 4e 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 17 78 03 00 00 00 00 00 17 78 03 00 00 00 00 00 00 00 00 00 00 00 00 00 42 69 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 3a fd 04 00 00 00 00	`<2|h+\BB? #`AZb@NxxBi@:	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	50906	5164	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 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 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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8047.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 09 00 00 fd 07 00 00 05 00 00 00 04 01 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 0c 00 00 26 fd 00 00 15 00 00 00 fd 01 00 00 54 11 00 00 16 00 00 00 fd 00 00 00 40 13 00 00	)T8T&T@	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2	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	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	84	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	<WERReportMetadata>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	128	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	<OSVersionInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	180	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	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	270	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	<Build>17134</Build>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	318	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	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	408	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	<Edition>Professional</Edition>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	478	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	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	620	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	<Revision>1</Revision>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	672	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	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	752	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	<Architecture>X64</Architecture>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	824	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	<LCID>1033</LCID>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	864	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	</OSVersionInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	916	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	<ProcessInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 31 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2100</Pid>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1002	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	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 30 00 34 00 33 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>40430</Uptime>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1230	78	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 30 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 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1316	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	<IptEnabled>0</IptEnabled>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1376	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	<ProcessVmInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1430	96	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 32 00 32 00 30 00 33 00 34 00 30 00 36 00 31 00 30 00 36 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22034 06106624 </PeakVirtualSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1536	80	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 32 00 32 00 30 00 33 00 34 00 30 00 35 00 36 00 35 00 36 00 30 00 36 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203405656064</VirtualSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1626	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 36 00 33 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1630</PageFaultCount>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1710	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 36 00 32 00 38 00 37 00 33 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>6287360</PeakWorkingSetSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1806	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1810	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1816	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 36 00 32 00 38 00 37 00 33 00 36 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>628736</WorkingSetSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1896	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1900	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	1906	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 30 00 33 00 32 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 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	<QuotaPeakPagedPoolUsage>103272</QuotaPeakPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2020	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2024	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2030	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 30 00 32 00 35 00 32 00 30 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	<QuotaPagedPoolUsage>102520</QuotaPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2128	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2132	2	09 00		success or wait	3	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2138	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 31 00 37 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>17664</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2262	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2266	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2272	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 31 00 36 00 31 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>16128</QuotaNonPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2380	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2384	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2390	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 31 00 33 00 35 00 35 00 37 00 37 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1355776</PagefileUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2466	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2470	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2476	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 31 00 33 00 36 00 33 00 39 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	<PeakPagefileUsage>1363968</PeakPagefileUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2568	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2572	2	09 00		success or wait	3	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2578	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 31 00 33 00 35 00 35 00 37 00 37 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1355776</PrivateUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2650	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2654	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2658	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	</ProcessVmInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2704	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2708	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2712	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	<ParentProcess>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2742	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2746	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2752	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	<ProcessInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2792	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2796	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2804	28	3c 00 50 00 69 00 64 00 3e 00 34 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>492</Pid>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2832	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2836	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2844	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 36 00 34 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	<ImageName>loaddll64.exe</ImageName>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2916	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2920	2	09 00		success or wait	4	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	2928	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3018	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3022	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3030	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 34 00 32 00 33 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>44230</Uptime>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3086	78	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 30 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 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3176	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	<IptEnabled>0</IptEnabled>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3240	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	<ProcessVmInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3298	90	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 34 00 33 00 34 00 35 00 31 00 31 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4345114624</PeakVirtualSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3402	74	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 34 00 33 00 34 00 31 00 34 00 35 00 32 00 38 00 30 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	<VirtualSize>4341452800</VirtualSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3476	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3480	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3490	72	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 36 00 38 00 34 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	<PageFaultCount>684</PageFaultCount>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3562	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3566	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3576	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 32 00 34 00 37 00 33 00 39 00 38 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	<PeakWorkingSetSize>2473984</PeakWorkingSetSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3672	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3676	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3686	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 32 00 34 00 37 00 33 00 39 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2473984</WorkingSetSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3780	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 36 00 39 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<QuotaPeakPagedPoolUsage>69648</QuotaPeakPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	3906	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 36 00 32 00 33 00 32 00 30 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	<QuotaPagedPoolUsage>62320</QuotaPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4016	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 34 00 30 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	<QuotaPeakNonPagedPoolUsage>4072</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4152	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 33 00 31 00 32 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 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>3120</QuotaNonPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4258	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4262	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4272	74	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 34 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>548864</PagefileUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4346	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4350	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4360	90	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 34 00 38 00 38 00 36 00 34 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	<PeakPagefileUsage>548864</PeakPagefileUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4450	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4454	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4464	70	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 34 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>548864</PrivateUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4534	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4538	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4546	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	</ProcessVmInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4592	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4596	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4602	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	</ProcessInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4644	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4648	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4652	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	</ParentProcess>	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4684	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4688	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4690	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	</ProcessInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4732	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4736	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4738	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	<ProblemSignatures>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4776	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4780	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4784	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	<EventType>APPCRASH</EventType>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4846	4	0d 00 0a 00		success or wait	8	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4850	2	09 00		success or wait	16	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	4854	104	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 5f 00 70 00 7a 00 47 00 30 00 72 00 6b 00 49 00 63 00 68 00 72 00 2e 00 64 00 6c 00 6c 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	<Parameter0>rundll32.exe_pzG0rklchr.dll</Parameter0>	success or wait	8	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	5510	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	5514	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	5516	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	</ProblemSignatures>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	5556	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	5560	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	5562	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	<DynamicSignatures>	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	5600	4	0d 00 0a 00		success or wait	6	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	5604	2	09 00		success or wait	12	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	5608	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	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6162	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6166	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6168	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	</DynamicSignatures>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6208	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6212	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6214	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	<SystemInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6252	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6256	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6260	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	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6354	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6358	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6362	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 6b 00 78 00 62 00 63 00 6b 00 6f 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	<SystemManufacturer>kxbcko, Inc.</SystemManufacturer>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6468	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6472	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6476	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 6b 00 78 00 62 00 63 00 6b 00 6f 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	<SystemProductName>kxbcko7,1</SystemProductName>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6572	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6576	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6580	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 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 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	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6700	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6704	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6708	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 36 00 32 00 36 00 33 00 33 00 36 00 35 00 35 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	<OSInstallDate>1626336554</OSInstallDate>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6790	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6794	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6798	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	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6900	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6904	2	09 00		success or wait	2	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6908	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6978	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6982	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	6984	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	</SystemInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7024	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7028	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7030	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	<SecureBootState>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7064	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7068	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7072	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	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7168	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7172	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7174	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	</SecureBootState>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7216	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	<Integrator>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7240	4	0d 00 0a 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7244	2	09 00		success or wait	6	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7248	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 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7502	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7506	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7508	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	</Integrator>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7534	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7538	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7540	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 32 00 2d 00 31 00 31 00 2d 00 32 00 34 00 54 00 30 00 34 00 3a 00 31 00 39 00 3a 00 34 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-24T04:19:46Z">	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7640	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7644	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7648	262	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 32 00 39 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 31 00 30 00 30 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 31 00 39 00 36 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 31 00 39 00 36 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 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="298" PID="2100" UptimeMS="1968" TimeSinceCreationMS="1968" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7910	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7914	2	09 00		success or wait	3	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	7920	188	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 31 00 39 00 33 00 33 00 37 00 32 00 31 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 30 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="19337216" TimelineUnitShift="12" Timeline="11011"/>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8108	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8112	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8116	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8136	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8140	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8142	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	</ProcessTimelines>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8180	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8184	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8186	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	<ReportInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8224	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8228	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8232	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 65 00 38 00 36 00 38 00 61 00 32 00 31 00 2d 00 64 00 33 00 33 00 61 00 2d 00 34 00 36 00 36 00 36 00 2d 00 62 00 32 00 65 00 66 00 2d 00 36 00 38 00 32 00 38 00 36 00 62 00 35 00 30 00 30 00 66 00 39 00 35 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5e868a21-d33a-4666-b2ef-68286b500f95</Guid>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8330	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8334	2	09 00		success or wait	2	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8338	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 32 00 2d 00 31 00 31 00 2d 00 32 00 34 00 54 00 30 00 34 00 3a 00 31 00 39 00 3a 00 34 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-11-24T04:19:46Z</CreationTime>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8436	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8440	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8442	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	</ReportInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8482	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER848E.tmp.WERInternalMetadata.xml	8486	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	</WERReportMetadata>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8589.tmp.xml	0	4733	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 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 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_5df03237c245e7792ae728ba7af47d1bed8c47f7_4f0e5919_16399239\Report.wer	0	2	fd fd		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_5df03237c245e7792ae728ba7af47d1bed8c47f7_4f0e5919_16399239\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	148	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_5df03237c245e7792ae728ba7af47d1bed8c47f7_4f0e5919_16399239\Report.wer	9238	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 33 00 39 00 30 00 30 00 33 00 30 00 34 00 32 00 37 00	MetadataHash=-390030427	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF88B84E3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	FileId	unicode	00002f34ccfdd8141aeee2e89ffb070ce239c7d00706	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LowerCaseLongPath	unicode	c:\windows\system32\rundll32.exe	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LongPathHash	unicode	rundll32.exe|c8d854bf61fafc41	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Name	unicode	rundll32.exe	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Publisher	unicode	microsoft corporation	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinFileVersion	unicode	10.0.17134.1	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinaryType	unicode	pe64_amd64	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductVersion	unicode	10.0.17134.1	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LinkDate	unicode	05/20/2093 18:03:41	success or wait	1	7FF88B871D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinProductVersion	unicode	10.0.17134.1	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Size	B	00 10 01 00 00 00 00 00	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Language	dword	1033	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsPeFile	dword	1	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsOsComponent	dword	1	success or wait	1	7FF88B871D2D	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 D0 3E DD E2 FF 7F 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 E2 9A 07 8C F8 7F 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FF88B8707CB	RegSetValueExW

Analysis Process: WerFault.exe PID: **5188**, Parent PID: **1308**

General

Target ID:	12
Start time:	05:19:23
Start date:	24/11/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 1308 -s 304
Imagebase:	0x7ff69db50000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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	7FF88B85527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8683.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8683.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_f6b0ff3966a3d6c74191edf638977ebb42334d7_4f0e5919_156d919c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_f6b0ff3966a3d6c74191edf638977ebb42334d7_4f0e5919_156d919c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF88B84E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8683.tmp	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8683.tmp.xml	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERF57.tmp.csv	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER11DA.tmp.txt	success or wait	1	7FF88B84E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd fd 7e 63 fd 05 12 00 00 00 00 00	MDMP ~c	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	5080	6	00 00 00 00 00 00		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	200	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 fd 13 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 35 fd 01 00 00 54 05 00 00 fd 03 00 00 1c 05 00 00 fd fd 7e 63 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 01 00 00 00 fd fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00	UBLwT~c0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	5750	1232	fd fd 61 1f fd 42 00 00 40 14 60 fd fd 7f 00 00 0a 00 00 00 00 00 00 00 7d 45 58 fd fd 7f 00 00 fd 00 05 00 00 00 00 00 fd 0b fd fd 2f 02 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 fd 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 76 12 05 00 00 00 00 00 fd 00 05 00 00 00 00 00 38 fd fd fd 00 00 00 00 0a 00 00 00 00 00 00 00 50 fd fd fd fd 00 00 00 fd 08 fd fd 00 00 00 00 2e 4c 03 fd 00 00 00 00 0e a7 fd 00 00 00 00 fd 53 03 fd 00 00 00 00 0a 00 00 00 00 00 00 00 fd 0f fd 11 fd 0f 00 00 fd fd fd fd fd 00 00 00 6f 53 03 fd 00 00 00 00 fd a7 fd 00 00 00 00 fd fd 04 00 00 00 00 00 49 12 00 00 00 00 00 00 40 7f 08 fd fd 7f 00	aB@`}EX/_3++S++v8P.LSoSI@	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	1620	168	48 0f 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 40 7f 08 fd fd 7f 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 76 16 00 00	H@v	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	10678	20	10 00 00 00 68 a7 fd fd 00 00 00 08 00 00 00 fd 2a 00 00	h*	success or wait	16	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	10938	8	fd fd 00 fd fd 7f 00 00		success or wait	15	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	41610	8192	00 00 00 00 00 00 00 00 00 00 fd fd fd 00 00 00 00 40 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 06 fd fd 00 00 00 00 00 00 00 00 00 00 00 1c 05 00 00 00 00 00 00 1c 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	1788	4	03 00 00 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	6982	1232	fd fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 78 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 78 fd fd fd 00 00 00 fd fd fd fd fd fd fd fd 78 a7 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 68 a7 fd fd 00 00 00 fd e7 fd fd 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 78 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 bf fd fd 7f 00	x 3++S++Fxxhx	success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	1888	48	1c 0c 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 06 fd fd 00 00 00 38 fd fd fd fd 00 00 00 fd 05 00 00 fd 54 00 00 fd 04 00 00 fd 24 00 00	8T$	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	1948	4	17 00 00 00		success or wait	23	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	5086	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	rundll32.exe	success or wait	23	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	4328	752	00 00 60 fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 5c 16 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 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 60 41 00 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 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 00 30 fd 02 00 00 00 00 00 fd 15 03 00 00 00 00 fd 4e 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 10 78 03 00 00 00 00 00 19 78 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 65 1b 00 00 00 00 00 4f fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 3a fd 04 00 00 00 00	`<2|h+\BB? #`AZb0NxxeO@:	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	49802	5164	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 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 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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER80D3.tmp.dmp	32	108	03 00 00 00 fd 00 00 00 fd 06 00 00 04 00 00 00 fd 09 00 00 fd 07 00 00 05 00 00 00 04 01 00 00 fd 29 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 0c 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 54 11 00 00 16 00 00 00 fd 00 00 00 40 13 00 00	)T8TT@	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2	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	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	84	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	<WERReportMetadata>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	128	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	<OSVersionInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	180	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	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	270	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	<Build>17134</Build>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	318	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	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	408	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	<Edition>Professional</Edition>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	478	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	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	620	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	<Revision>1</Revision>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	672	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	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	752	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	<Architecture>X64</Architecture>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	824	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	<LCID>1033</LCID>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	864	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	</OSVersionInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	916	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	<ProcessInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 31 00 33 00 30 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1308</Pid>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1002	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	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000000</CmdLineSignature>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 36 00 30 00 30 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>36005</Uptime>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1230	78	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 30 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 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1316	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	<IptEnabled>0</IptEnabled>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1376	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	<ProcessVmInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1430	96	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 32 00 32 00 30 00 33 00 34 00 30 00 36 00 31 00 30 00 36 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203406106624</PeakVirtualSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1536	80	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 32 00 32 00 30 00 33 00 34 00 30 00 35 00 36 00 35 00 36 00 30 00 36 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203405656064</VirtualSize>	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1626	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 36 00 33 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1633</PageFaultCount>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1710	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 36 00 32 00 39 00 35 00 35 00 35 00 32 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	<PeakWorkingSetSize>6295552</PeakWorkingSetSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1806	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1810	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1816	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 36 00 32 00 39 00 35 00 35 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6295552</WorkingSetSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1896	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1900	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	1906	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 30 00 33 00 32 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 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	<QuotaPeakPagedPoolUsage>103272</QuotaPeakPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2020	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2024	2	09 00		success or wait	3	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2030	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 30 00 32 00 35 00 32 00 30 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	<QuotaPagedPoolUsage>102520</QuotaPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2128	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2132	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2138	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 31 00 37 00 36 00 39 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 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	<QuotaPeakNonPagedPoolUsage>17696</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2262	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2266	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2272	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 31 00 36 00 31 00 36 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 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>16160</QuotaNonPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2380	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2384	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2390	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 31 00 33 00 36 00 33 00 39 00 36 00 38 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	<PagefileUsage>1363968</PagefileUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2466	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2470	2	09 00		success or wait	3	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2476	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 31 00 33 00 37 00 32 00 31 00 36 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>13 72160</Pe akPagefileUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2568	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2572	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2578	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 31 00 33 00 36 00 33 00 39 00 36 00 38 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	<PrivateUsage>1363968 </PrivateUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2650	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2654	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2658	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	</ProcessVmInformation >	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2704	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2708	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2712	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	<ParentProcess>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2742	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2746	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2752	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	<ProcessInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2792	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2796	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2804	28	3c 00 50 00 69 00 64 00 3e 00 34 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>492</Pid>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2832	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2836	2	09 00		success or wait	4	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2844	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 36 00 34 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	<ImageName>loaddll64.exe</ImageName>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2916	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2920	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	2928	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>000000</CmdLineSignature>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3018	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3022	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3030	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 34 00 34 00 36 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>44461</Uptime>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3086	78	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 30 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 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3176	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	<IptEnabled>0</IptEnabled>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3240	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	<ProcessVmInformation>	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3298	90	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 34 00 33 00 34 00 35 00 31 00 31 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4345114624</PeakVirtualSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3402	74	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 34 00 33 00 34 00 31 00 34 00 35 00 32 00 38 00 30 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	<VirtualSize>4341452800</VirtualSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3476	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3480	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3490	72	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 36 00 38 00 34 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	<PageFaultCount>684</PageFaultCount>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3562	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3566	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3576	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 32 00 34 00 37 00 33 00 39 00 38 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	<PeakWorkingSetSize>2473984</PeakWorkingSetSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3672	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3676	2	09 00		success or wait	5	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3686	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 32 00 34 00 37 00 33 00 39 00 38 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2473984</WorkingSetSize>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3766	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3770	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3780	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 36 00 39 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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	<QuotaPeakPagedPoolUsage>69648</QuotaPeakPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3892	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3896	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	3906	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 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 36 00 32 00 33 00 32 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	<QuotaPagedPoolUsage>62320</QuotaPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4002	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4006	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4016	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 34 00 30 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	<QuotaPeakNonPagedPoolUsage>4072</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4138	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4142	2	09 00		success or wait	5	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4152	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 33 00 31 00 32 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 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>3120</QuotaNonPagedPoolUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4258	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4262	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4272	74	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 34 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>548864</PagefileUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4346	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4350	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4360	90	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 34 00 38 00 38 00 36 00 34 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	<PeakPagefileUsage>548864</PeakPagefileUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4450	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4454	2	09 00		success or wait	5	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4464	70	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 34 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>548864</PrivateUsage>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4534	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4538	2	09 00		success or wait	4	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4546	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	</ProcessVmInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4592	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4596	2	09 00		success or wait	3	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4602	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	</ProcessInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4644	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4648	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4652	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	</ParentProcess>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4684	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4688	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4690	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	</ProcessInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4732	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4736	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4738	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	<ProblemSignatures>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4776	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4780	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4784	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	<EventType>APPCRASH</EventType>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4846	4	0d 00 0a 00		success or wait	8	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4850	2	09 00		success or wait	16	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	4854	104	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 5f 00 70 00 7a 00 47 00 30 00 72 00 6b 00 49 00 63 00 68 00 72 00 2e 00 64 00 6c 00 6c 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	<Parameter0>rundll32.exe_pzG0rkIchr.dll</Parameter0>	success or wait	8	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	5510	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	5514	2	09 00		success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	5516	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	</ProblemSignatures>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	5556	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	5560	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	5562	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	<DynamicSignatures>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	5600	4	0d 00 0a 00		success or wait	6	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	5604	2	09 00		success or wait	12	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	5608	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	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6162	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6166	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6168	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	</DynamicSignatures>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6208	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6212	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6214	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	<SystemInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6252	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6256	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6260	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	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6354	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6358	2	09 00		success or wait	2	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6362	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 6b 00 78 00 62 00 63 00 6b 00 6f 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	<SystemManufacturer>kxbcko, Inc.</SystemManufacturer>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6468	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6472	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6476	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 6b 00 78 00 62 00 63 00 6b 00 6f 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	<SystemProductName>kxbcko7,1</SystemProductName>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6572	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6576	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6580	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 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 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	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6700	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6704	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6708	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 36 00 32 00 36 00 33 00 33 00 36 00 35 00 35 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	<OSInstallDate>1626336554</OSInstallDate>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6790	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6794	2	09 00		success or wait	2	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6798	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	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6900	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6904	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6908	70	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 2d 00 30 00 31 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>-01:00</TimeZoneBias>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6978	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6982	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	6984	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	</SystemInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7024	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7028	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7030	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	<SecureBootState>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7064	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7068	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7072	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	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7168	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7172	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7174	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	</SecureBootState>	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7210	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7214	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7216	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	<Integrator>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7240	4	0d 00 0a 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7244	2	09 00		success or wait	6	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7248	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 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7502	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7506	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7508	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	</Integrator>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7534	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7538	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7540	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 32 00 2d 00 31 00 31 00 2d 00 32 00 34 00 54 00 30 00 34 00 3a 00 31 00 39 00 3a 00 34 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-24T04:19:46Z">	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7640	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7644	2	09 00		success or wait	2	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7648	262	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 30 00 31 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 33 00 30 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 39 00 32 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 39 00 32 00 31 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 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="301" PID="1308" UptimeMS="2921" TimeSinceCreationMS="2921" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7910	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7914	2	09 00		success or wait	3	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	7920	186	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 31 00 39 00 33 00 33 00 37 00 32 00 31 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 30 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="19337216" TimelineUnitShift="12" Timeline="1011"/>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8106	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8110	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8114	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8134	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8138	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8140	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	</ProcessTimelines>	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8178	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8182	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8184	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	<ReportInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8222	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8226	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8230	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 62 00 31 00 62 00 30 00 37 00 34 00 65 00 2d 00 33 00 31 00 62 00 35 00 2d 00 34 00 34 00 32 00 36 00 2d 00 39 00 39 00 61 00 35 00 2d 00 39 00 39 00 35 00 64 00 64 00 33 00 64 00 38 00 34 00 63 00 38 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>9b1b074e-31b5-4426-99a5-995dd3d84c84</Guid>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8328	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8332	2	09 00		success or wait	2	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8336	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 32 00 2d 00 31 00 31 00 2d 00 32 00 34 00 54 00 30 00 34 00 3a 00 31 00 39 00 3a 00 34 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-11-24T04:19:46Z</CreationTime>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8434	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8438	2	09 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8440	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	</ReportInformation>	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8480	4	0d 00 0a 00		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8588.tmp.WERInternalMetadata.xml	8484	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	</WERReportMetadata>	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER8683.tmp.xml	0	4733	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 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 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_f6b0ff3966a3d6c74191edf638977ebb42334d7_4f0e5919_156d919c\Report.wer	0	2	fd fd		success or wait	1	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_f6b0ff3966a3d6c74191edf638977ebb42334d7_4f0e5919_156d919c\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	148	7FF88B84E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_f6b0ff3966a3d6c74191edf638977ebb42334d7_4f0e5919_156d919c\Report.wer	9238	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 31 00 36 00 38 00 31 00 31 00 34 00 34 00 34 00 31 00	MetadataHash=-1168114441	success or wait	1	7FF88B84E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF88B871D2D	unknown
\REGISTRY\A\{a8654e0f-a976-e283-25ad-ac4613afc19f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF88B84E3FE	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 E2 9A 07 8C F8 7F 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 00 40 7F 08 8C F8 7F 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 E2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FF88B8707CB	RegSetValueExW

Analysis Process: WerFault.exe PID: **5968**, Parent PID: **2100**

General	
Target ID:	13
Start time:	05:19:27
Start date:	24/11/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 2100 -s 304
Imagebase:	0x7ff69db50000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **3260**, Parent PID: **1308**

General	
Target ID:	14
Start time:	05:19:42
Start date:	24/11/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 1308 -s 304
Imagebase:	0x7ff69db50000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly