ID: 752975
Sample Name: pzG0rkIchr.dll
Cookbook: default.jbs
Time: 05:29:36
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report pzG0rkIchr.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
E-Banking Fraud 6
Hooking and other Techniques for Hiding and Protection 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 12
Public IPs 12
Private 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASNs 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_206411b7d18c8b51ef308e99261d801f59953bc0_4f0e5919_15ebd55f\Report.wer 14
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_738eef979a666465c6051ddd5fef4b7e70c91a_4f0e5919_15905d59\Report.wer
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml 1414
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BBF.tmp.xml 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD021.tmp.xml 15
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp 16
Static File Info 16
General 16
File Icon 16
Static PE Info 17
General 17
Authenticode Signature 17
Entrypoint Preview 17
Rich Headers 19
Data Directories 19
Sections 19
Imports 19
Exports 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 20
TCP Packets 21
UDP Packets 22
DNS Queries 22
DNS Answers 23
Statistics 23
Behavior 23
System Behavior 23

Analysis Process: loaddll64.exePID: 1556, Parent PID: 3452 23
General 23
File Activities 24
Analysis Process: conhost.exePID: 4696, Parent PID: 1556 24
General 24
Analysis Process: cmd.exePID: 1076, Parent PID: 1556 24
General 24
File Activities 24
Analysis Process: regsvr32.exePID: 2356, Parent PID: 1556 24
General 24
File Activities 25
Analysis Process: rundll32.exePID: 5268, Parent PID: 1076 25
General 25
Analysis Process: rundll32.exePID: 5264, Parent PID: 1556 25
General 25
Analysis Process: rundll32.exePID: 6044, Parent PID: 1556 25
General 25
Analysis Process: rundll32.exePID: 6136, Parent PID: 1556 26
General 26
Analysis Process: WerFault.exePID: 5572, Parent PID: 6044 26
General 26
File Activities 26
File Created 26
File Deleted 27
File Written 27
Registry Activities 49
Key Created 49
Key Value Created 49
Key Value Modified 50
Analysis Process: WerFault.exePID: 5404, Parent PID: 6136 51
General 51
File Activities 51
File Created 51
File Deleted 52
File Written 52
Registry Activities 74
Key Created 74
Key Value Modified 74
Analysis Process: WerFault.exePID: 680, Parent PID: 6136 75
General 75
Disassembly 75

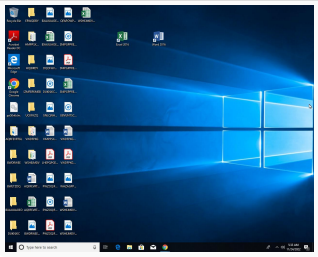
Windows Analysis Report

pzG0rkIchr.dll

Overview

General Information

Sample Name:	pzG0rkIchr.dll
Analysis ID:	752975
MD5:	d6ef4778f7dc9c3..
SHA1:	5dad8394ef37d5..
SHA256:	54de1f2c26a63a..
Tags:	exe LDR4
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

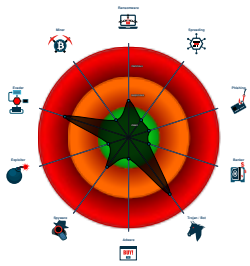
Ursnif

Score:	92
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
- Multi AV Scanner detection for dom…
- 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

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 1556 cmdline: loaddll64.exe "C:\Users\user\Desktop\pzG0rkIchr.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 4696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 1076 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\pzG0rkIchr.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5268 cmdline: rundll32.exe "C:\Users\user\Desktop\pzG0rkIchr.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 2356 cmdline: regsvr32.exe /s C:\Users\user\Desktop\pzG0rkIchr.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 5264 cmdline: rundll32.exe C:\Users\user\Desktop\pzG0rkIchr.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6044 cmdline: rundll32.exe C:\Users\user\Desktop\pzG0rkIchr.dll,ItsnPq5v MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 5572 cmdline: C:\Windows\system32\WerFault.exe -u -p 6044 -s 276 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 6136 cmdline: rundll32.exe C:\Users\user\Desktop\pzG0rkIchr.dll,QlqYo259k MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 5404 cmdline: C:\Windows\system32\WerFault.exe -u -p 6136 -s 304 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - WerFault.exe (PID: 680 cmdline: C:\Windows\system32\WerFault.exe -u -p 6136 -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: 1556	JoeSecurity_Ursnif_v4	Yara detected Ursnif	Joe Security	
Process Memory Space: regsvr32.exe PID: 2356	JoeSecurity_Ursnif_v4	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 5268	JoeSecurity_Ursnif_v4	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 5264	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

Multi AV Scanner detection for domain / URL

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

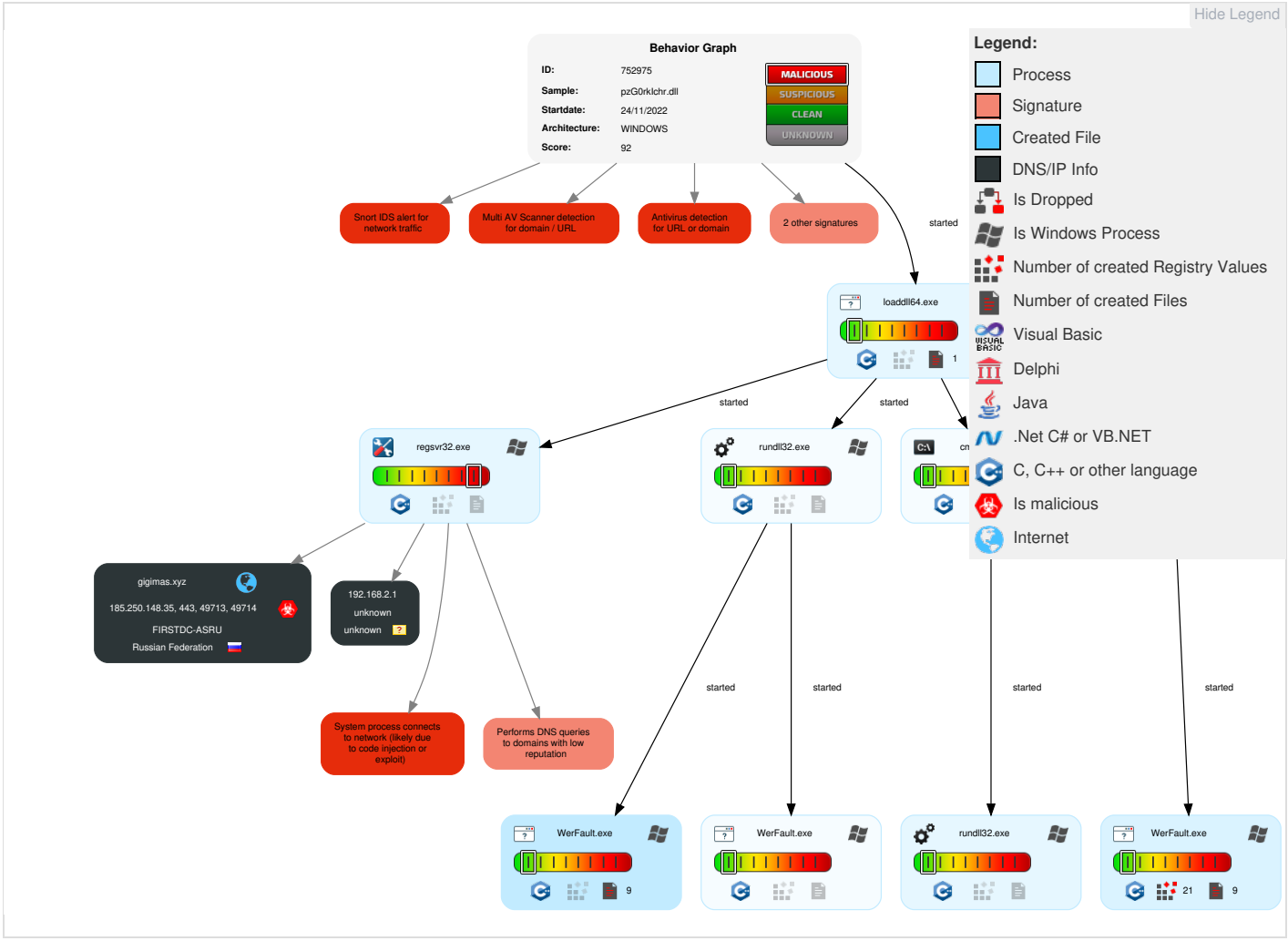
Yara detected Ursnif

Yara detected Ursnif

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

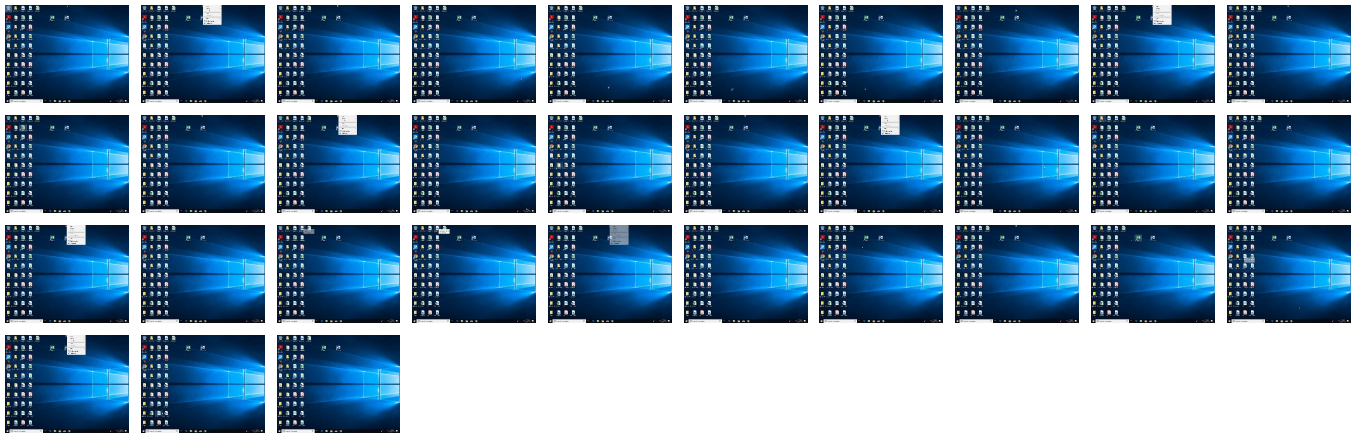
Behavior Graph



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	57%	Virustotal		Browse
pzG0rklchr.dll	73%	ReversingLabs	Win64.Trojan.Tnega	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
gigimas.xyz	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://gigimas.xyz	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://gigimas.xyz	11%	Virustotal		Browse
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
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://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/index.html9Pu/JI	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/index.html5F	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/index.html	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/index.htmlT	0%	Avira URL Cloud	safe	
http://https://Mozilla/5.0	0%	Avira URL Cloud	safe	
http://https://gigimas.xyzhttps://reaso.xyz	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz/index.htmlm	0%	Avira URL Cloud	safe	
http://https://gigimas.xyz:443/index.htmlY_	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://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	• 14%, Virustotal, Browse	unknown

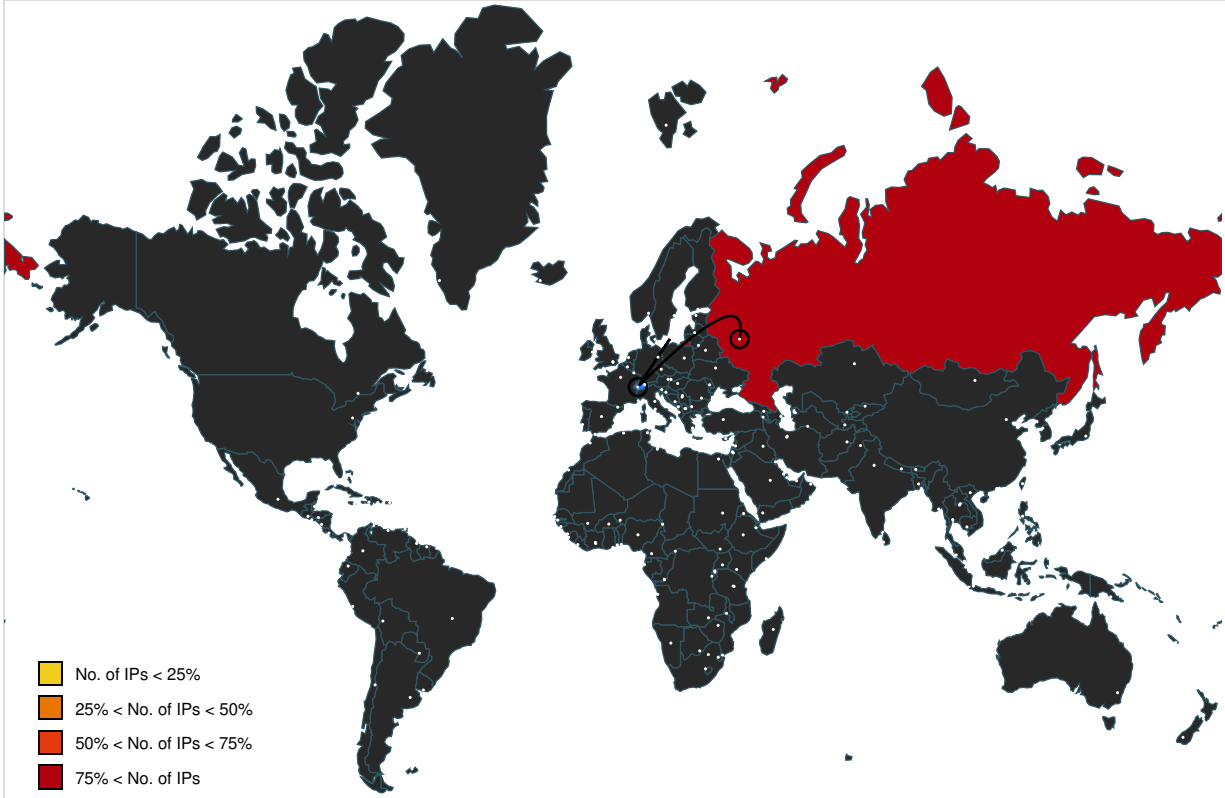
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gigimas.xyz	loaddll64.exe, 00000000.00000003.631018067.000002016434000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.641761210.00000000021BD000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.641543041.00000000020E0000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.357258070.0000017B374A0000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000003.357488590.00000201A4290000.00000004.00000020.00020000.00000000.sdmp	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	pzG0rklchr.dll	false	• URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	pzG0rklchr.dll	false	• URL Reputation: safe	unknown
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	pzG0rklchr.dll	false	• URL Reputation: safe	unknown
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	pzG0rklchr.dll	false	• URL Reputation: safe	unknown
http://ocsp.sectigo.com0	pzG0rklchr.dll	false	• URL Reputation: safe	unknown
http://https://gigimas.xyz/index.html9Pu/JI	regsvr32.exe, 00000003.00000003.466312748.00000000007DD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://gigimas.xyz/index.html5F	regsvr32.exe, 00000003.00000003.596495160.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.641359278.00000000007E8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://Mozilla/5.0	loaddll64.exe, 00000000.00000003.631032238.0000020164342000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.641554871.00000000020E2000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.357262173.0000017B374A2000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000003.357492545.00000201A4292000.00000004.00000020.00020000.00000000.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	regsvr32.exe, 00000003.00000003.466330233.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.596506826.000000000078D000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.596495160.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.531293534.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.641359278.00000000007E8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://gigimas.xyz/index.htmlT	regsvr32.exe, 00000003.00000002.641214444.00000000007C6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.596466270.00000000007C6000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.531265696.00000000007C6000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http://https://gigimas.xyzhttps://reaso.xyz	regsvr32.exe, 00000003.00000002.641761210.00000000021BD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://gigimas.xyz/index.htmlm	regsvr32.exe, 00000003.00000002.641004710.0000000000785000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	pzG0rkIchr.dll	false	• URL Reputation: safe	unknown
http://https://gigimas.xyz/	regsvr32.exe, 00000003.00000003.466330233.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.596495160.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.595788178.0000000000815000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.531293534.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.641484903.0000000000813000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.596407001.0000000000813000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.641359278.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000003.466249755.00000000007A9000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://gigimas.xyz:443/index.htmlY_	regsvr32.exe, 00000003.00000003.596495160.00000000007E8000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.641359278.00000000007E8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://reaso.xyz	regsvr32.exe, 00000003.00000002.641761210.00000000021BD000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000003.00000002.641543041.00000000020E0000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000004.00000003.357258070.0000017B374A0000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000005.00000003.357488590.00000201A4290000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://gigimas.xyz:443/index.html	regsvr32.exe, 00000003.00000003.531293534.00000000007E8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	752975
Start date and time:	2022-11-24 05:29:36 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pzG0rklchr.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	25
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:	mal92.troj.evad.winDLL@19/8@4/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 78% (good quality ratio 69.5%) • Quality average: 59.8% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.42.65.92
- Excluded domains from analysis (whitelisted): fs.microsoft.com, onedsblobprdeus17.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, ctldl.windowsupdate.com, 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.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

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_206411b7d18c8b51ef308e99261d801f59953bc0_4f0e5919_15ebd55f\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):	0.7599332074807373
Encrypted:	false
SSDEEP:	96:YImFIZZFiWpJPnyijs55P7HfgpXIQcQdc6/RcENcw3VXaXz+HbHgSQgJPbJIDV9+:nm3FiYJKgHz9XpjEI/u7sGOS274ltC
MD5:	4D7AD4D16E977190A93A4217F65D5552
SHA1:	4C633364E29B27CC5520425ACF90D722D0615F55
SHA-256:	538A208795EC006468C02E86FF3F447417F354986183D6CF0BB1202C6DCD6B33
SHA-512:	E9A45DA51EF7DB62A595D2FA006C1FD4E4E2B307822E7AED13001CA6517DBFDA7B4D9ECB4B77B11784C4F5ADA883C7DB69F9E028D3C6D9B95023BD486973E102
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.=.1.3.3.1.3.7.7.0.2.8.9.3.4.1.7.5.1.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.1.3.7.7.0.2.9.0.4.3.5.3.8.3.7.....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.=.5.4.5.a.7.c.8.e.-.c.e.f.3.-.4.d.d.a.-.9.e.b.5.-.3.1.5.6.4.a.f.2.e.c.5.c.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.e.c.2.f.5.9.5.-.e.a.9.0.-.4.6.7.7.-.b.6.a.3.-.f.0.b.e.2.d.9.9.5.5.b.5.....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.=.0.0.0.0.1.7.f.8.-.0.0.0.1.-.0.0.1.f.-.2.0.5.2.-.d.3.f.1.0.8.0.0.d.9.0.1.....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_738eef979a666465c6051ddd5fef4b7e70c91a_4f0e5919_15905d59\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):	0.7588806812185113
Encrypted:	false
SSDEEP:	96:EtaFiDJPnycjs551DW9SspXIQcQQGc6bcEKcw3UUeXaXz+HbHgSQgJPbph88WpOX:sciDJKWH1fQ4Ucjpe/u7sGOS274lt9
MD5:	970AE762D984AB0562EF2DDEE4F7F71C
SHA1:	BB145548E992EC8183CD51D92E4C3494DE7B0EC1
SHA-256:	402CD5EB9A3A996EB553A8C5485895A3AD576D1556CCCB08E20366B7A3C00A40
SHA-512:	794C6926A380144449AA7C24BA1407D67EA8A41F89ABAD333313D324799DBC1F4C76D52F49A91D112AF60FCA87CA01F12F0F7648B4AAB095A5AB367A8DDE84AA
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.6.4.....E.v.e.n.t.T.i.m.e.=.1.3.3.1.3.7.7.0.2.5.5.9.0.6.7.1.6.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.1.3.7.7.0.2.7.4.4.0.6.6.7.6.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.6.5.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.9.e.6.c.7.3.8.-.b.f.f.7.-.4.b.6.8.-.b.7.e.a.-.0.d.5.0.5.d.9.5.7.9.4.d...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.=.7.4.9.2.a.f.f.d.-.7.3.5.e.-.4.c.a.7.-.a.0.e.b.-.9.9.7.a.b.a.e.1.b.4.1.4.....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.=.0.0.0.0.1.7.9.c.-.0.0.0.1.-.0.0.1.f.-.0.3.9.0.-.a.1.e.e.0.8.0.0.d.9.0.1.....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.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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):	8606
Entropy (8bit):	3.6917131740684326
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNibXpiH6YmObgmf9lpSDUf9CpDz89bv7QfAFm:RrlsNiLpiH6Yvbgmf9lpSWv8fv
MD5:	A25026BF04BD3F85B66322DD4EACE463
SHA1:	3E6F42AACBDC7749C351F4040836974F0FE849E8
SHA-256:	EF29167FAC14085CEDC2B51E3DD871909F41CF22CD799EE08F16E10BC5F25340
SHA-512:	7AF918F7B179540C5C0250F8E7C698AEFA2B7873F29B792D886EA8256C447CA561DA47EC2668FB3972F8F954F438D84DF8C98E8C447248C17C7FD927D4793FD3
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.>.6.0.4.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BBF.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4852
Entropy (8bit):	4.453732860738506
Encrypted:	false
SSDEEP:	48:cvIwSD8zs/JgtBl9C0Wgc8sqYjHs8fm8M4JCXCODFSoyq8vhObZESC5S6d:uITfhEtgrsqYTRJeWqVv6d
MD5:	36514A65B9F12B58AFD0BBEC14BB306B
SHA1:	708D342C0B5E7C27C165196A66BA72199935C035
SHA-256:	1E2FDEB64300A379966992E05CDCED721176C203B2AEA77D8521699282520391
SHA-512:	0042E849F66066FE1C66E48516FCD7B735C49DB80A33C73C025965CC1544002AD8246D1716241A37BD1855EF92F2DB6540A3373E1D7E89B58447CAD2420BA6A9
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="1794161" />.. <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\WERCC66.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Nov 24 13:31:29 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	57126
Entropy (8bit):	1.6752029810543265
Encrypted:	false
SSDEEP:	192:QRENUeRlXOC5Ky21na9OBQpyomWlAgh0l:XeC0VQ9Oupy
MD5:	15A22FD2F4CA8ECE4C09E779E8BF5301
SHA1:	CF2A33C45D5845C636A662FBC221FF128EFFE3D2
SHA-256:	32AE357A2D002F95865AC8D24FA48BEEC756DF4547D071DA783E4676C7DE6702
SHA-512:	532611BDCDEE7F036330CAEB750CA8681D325436E10FF99A3F12B55C97ABC60D206C7105F426E3E76A10F88F9B2EE8D5C000E752DEDA295729A94B0DC84161D6
Malicious:	false
Preview:	MDMP..... .....1r.c.....).....T.....8.....T.....F.....T.....@.....U.....B.....Lw..... .....T.....r.c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...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\WERCF55.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):	8528
Entropy (8bit):	3.6927747114398133
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiXByMiO6Ymf7lay5gmfQeSiR9CprRA89bNz14fsDvm:RrlsNixNiO6YOngmfQeSh9NzafI
MD5:	62C5858D004322A987DA836EAAFCF3D0
SHA1:	92F1D11A4FFAF0BC607AD9D80B0733B9C0AF776C
SHA-256:	E4ADEDF6BDB44F7A887C8FAEFA13E8932F54043F510FC6E6F6C9AD763A3D5E0E
SHA-512:	2244B303A7B773AE32265E693A04F0DA0A6A1BD91CF90B58BD31F51770ECA29D0D7A8DEB1E80090473442B0E03FCDBAB3F6A377970F38D5F9211160FD773968
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.>.6.1.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD021.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):	4.475037901948798
Encrypted:	false
SSDEEP:	48:cvIwSD8zsKJgtBl9C0Wgc8sqYjK8fm8M4JCXCO/Flyq85m2knZESC5Sgd:uITfYEtgrsqYLJCTnVvgd
MD5:	B4E9E6B35D1BFAE0CB99ADA1D8BA4FB0
SHA1:	000AD3F75949E7EB512EA021578BBCF408B9AB13
SHA-256:	256C84BFDE399833C36F0B05ED98CD72BC1507AE7C28D6DE773C33253673138B
SHA-512:	A55F7E52226C64C2A45E23FA853E1DA40F9D8DC41F8488A1F634AEB597EE0EE61056CC453C7AAA61B35751E720B0504EA500D7A0FE7652D988AC45BBACE39349
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="1794162" />.. <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\WERDC43.tmp.dmp	
Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Nov 24 13:31:09 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	31470
Entropy (8bit):	2.120966153641428
Encrypted:	false
SSDEEP:	96:5U8oyl8/7PSDKwNULtCTy+poi7C5VZ5ro8189EzF5oFPV4sGvTWIXmIf4ywMGVl9:FoyWocCTyOC5KwzzoAtkUWa
MD5:	53678B23171E44FF503435C4B6EE4E82
SHA1:	CBBF51D8D6EC4215E00C23AE2CB2DDEE3D01CF47
SHA-256:	EBE61E60D7251461BAA6A84830EBD1CA17739D2616F7DB1BD0555EBCE7BE7F4A
SHA-512:	EAFB2D40ACE89BDF7B02C147E9C69D9FADEBD0000C1260C46078197DA96E561B571A5BEC7D653A614A8BAEE730299C8F78C5FA7380557B3F3D86542FA0324D6A
Malicious:	false
Preview:	MDMP..... .....r.c.....4.....L...H.....$.....T...z.....`.....8.....T.....(....o.....U.....B.....<.... ...Lw.....T.....q.c.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...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..... ....

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	• 7/5/2021 5:00:00 PM 7/6/2022 4:59:59 PM
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 00007FBFC4794AE7h
call 00007FBFC4794EE0h
dec esp
mov eax, edi
mov edx, ebx
dec eax

Instruction
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 00007FBFC479495Ch
int3
int3
int3
dec eax
sub esp, 28h
call 00007FBFC4795378h
test eax, eax
je 00007FBFC4794B03h
dec eax
mov eax, dword ptr [00000030h]
dec eax
mov ecx, dword ptr [eax+08h]
jmp 00007FBFC4794AE7h
dec eax
cmp ecx, eax
je 00007FBFC4794AF6h
xor eax, eax
dec eax
cmpxchg dword ptr [00038A68h], ecx
jne 00007FBFC4794AD0h
xor al, al
dec eax
add esp, 28h
ret
mov al, 01h
jmp 00007FBFC4794AD9h
int3
int3
int3
dec eax
sub esp, 28h
call 00007FBFC479533Ch
test eax, eax
je 00007FBFC4794AE9h
call 00007FBFC479515Fh
jmp 00007FBFC4794AFBh
call 00007FBFC4795324h
mov ecx, eax
call 00007FBFC4796A91h
test eax, eax
je 00007FBFC4794AE6h
xor al, al
jmp 00007FBFC4794AE9h
call 00007FBFC4796E18h
mov al, 01h
dec eax
add esp, 28h
ret
dec eax
sub esp, 28h

Instruction
xor ecx, ecx
call 00007FBFC4794C26h
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

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

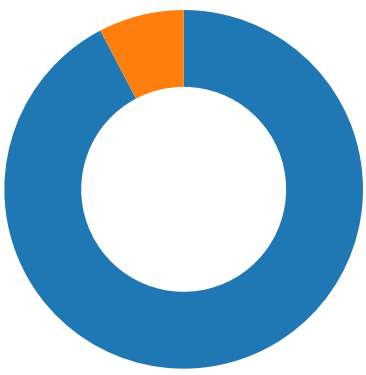
Name	Ordinal	Address
DllRegisterServer	1	0x180002380
ItsnPq5v	2	0x180002390
QlqYo259k	3	0x180017c20
XeFnYZ409	4	0x1800175e0

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



Total Packets: 52

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 05:31:42.779120922 CET	49713	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.779216051 CET	443	49713	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.779381990 CET	49713	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.783556938 CET	49713	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.783611059 CET	443	49713	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.841033936 CET	443	49713	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.848084927 CET	49714	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.848155022 CET	443	49714	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.848277092 CET	49714	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.849534035 CET	49714	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.849570036 CET	443	49714	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.906461954 CET	443	49714	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.909106970 CET	49715	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.909188032 CET	443	49715	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.910044909 CET	49715	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.910046101 CET	49715	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.910130024 CET	443	49715	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.965094090 CET	443	49715	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.970076084 CET	49716	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.970132113 CET	443	49716	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:42.970264912 CET	49716	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.971513033 CET	49716	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:31:42.971546888 CET	443	49716	185.250.148.35	192.168.2.3
Nov 24, 2022 05:31:43.027291059 CET	443	49716	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.139549971 CET	49717	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.139607906 CET	443	49717	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.139703989 CET	49717	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.140322924 CET	49717	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.140345097 CET	443	49717	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.197118044 CET	443	49717	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.198286057 CET	49718	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.198349953 CET	443	49718	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.198457003 CET	49718	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.198988914 CET	49718	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.199012041 CET	443	49718	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.256309032 CET	443	49718	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.257666111 CET	49719	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.257718086 CET	443	49719	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.257812023 CET	49719	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.258507013 CET	49719	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.258538961 CET	443	49719	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.315129042 CET	443	49719	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.322362900 CET	49720	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.322433949 CET	443	49720	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.322513103 CET	49720	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.323424101 CET	49720	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:13.323457956 CET	443	49720	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:13.379005909 CET	443	49720	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.484684944 CET	49721	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.484752893 CET	443	49721	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.484850883 CET	49721	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.485667944 CET	49721	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.485697031 CET	443	49721	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.541486025 CET	443	49721	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.542974949 CET	49722	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.543049097 CET	443	49722	185.250.148.35	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 05:32:43.543201923 CET	49722	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.543780088 CET	49722	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.543811083 CET	443	49722	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.601726055 CET	443	49722	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.611546993 CET	49723	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.611643076 CET	443	49723	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.611826897 CET	49723	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.612270117 CET	49723	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.612310886 CET	443	49723	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.669603109 CET	443	49723	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.671479940 CET	49724	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.671566963 CET	443	49724	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.671897888 CET	49724	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.672238111 CET	49724	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:32:43.672307014 CET	443	49724	185.250.148.35	192.168.2.3
Nov 24, 2022 05:32:43.729829073 CET	443	49724	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:13.901851892 CET	49725	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:13.901915073 CET	443	49725	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:13.902000904 CET	49725	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:13.902689934 CET	49725	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:13.902705908 CET	443	49725	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:13.958076000 CET	443	49725	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:13.960711002 CET	49726	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:13.960813999 CET	443	49726	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:13.961004019 CET	49726	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:13.962261915 CET	49726	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:13.962327957 CET	443	49726	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:14.020241976 CET	443	49726	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:14.022346973 CET	49727	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:14.022407055 CET	443	49727	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:14.022514105 CET	49727	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:14.023082972 CET	49727	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:14.023117065 CET	443	49727	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:14.079648018 CET	443	49727	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:14.083456993 CET	49728	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:14.083499908 CET	443	49728	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:14.083667040 CET	49728	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:14.084922075 CET	49728	443	192.168.2.3	185.250.148.35
Nov 24, 2022 05:33:14.084939003 CET	443	49728	185.250.148.35	192.168.2.3
Nov 24, 2022 05:33:14.142575026 CET	443	49728	185.250.148.35	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 05:31:42.716654062 CET	53975	53	192.168.2.3	8.8.8.8
Nov 24, 2022 05:31:42.749726057 CET	53	53975	8.8.8.8	192.168.2.3
Nov 24, 2022 05:32:13.117352009 CET	51139	53	192.168.2.3	8.8.8.8
Nov 24, 2022 05:32:13.137461901 CET	53	51139	8.8.8.8	192.168.2.3
Nov 24, 2022 05:32:43.461288929 CET	52955	53	192.168.2.3	8.8.8.8
Nov 24, 2022 05:32:43.481966019 CET	53	52955	8.8.8.8	192.168.2.3
Nov 24, 2022 05:33:13.880306959 CET	60582	53	192.168.2.3	8.8.8.8
Nov 24, 2022 05:33:13.900351048 CET	53	60582	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 05:31:42.716654062 CET	192.168.2.3	8.8.8.8	0xefb3	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:32:13.117352009 CET	192.168.2.3	8.8.8.8	0x493d	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false

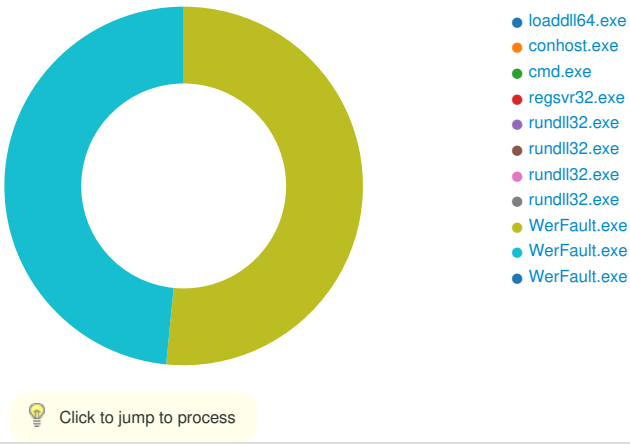
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 24, 2022 05:32:43.461288929 CET	192.168.2.3	8.8.8.8	0x7cb8	Standard query (0)	gigimas.xyz	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:33:13.880306959 CET	192.168.2.3	8.8.8.8	0xb47a	Standard query (0)	gigimas.xyz	A (IP 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 05:31:42.749726057 CET	8.8.8.8	192.168.2.3	0xefb3	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:32:13.137461901 CET	8.8.8.8	192.168.2.3	0x493d	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:32:43.481966019 CET	8.8.8.8	192.168.2.3	0x7cb8	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false
Nov 24, 2022 05:33:13.900351048 CET	8.8.8.8	192.168.2.3	0xb47a	No error (0)	gigimas.xyz		185.250.148.35	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **1556**, Parent PID: **3452**

General

Target ID:	0
Start time:	05:30:30
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:	0x7ff719eb0000
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: **4696**, Parent PID: **1556**

General	
Target ID:	1
Start time:	05:30:31
Start date:	24/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **1076**, Parent PID: **1556**

General	
Target ID:	2
Start time:	05:30:31
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:	0x7ff707bb0000
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: **2356**, Parent PID: **1556**

General	
Target ID:	3
Start time:	05:30:31
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:	0x7ff64da50000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
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: 5268, Parent PID: 1076

General

Target ID:	4
Start time:	05:30:31
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:	0x7ff6f9b90000
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: 5264, Parent PID: 1556

General

Target ID:	5
Start time:	05:30:31
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:	0x7ff6f9b90000
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: 6044, Parent PID: 1556

General

Target ID:	6
Start time:	05:30:36
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:	0x7ff6f9b90000
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: **6136**, Parent PID: **1556**

General

Target ID:	8
Start time:	05:30:40
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:	0x7ff6f9b90000
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: WerFault.exe PID: **5572**, Parent PID: **6044**

General

Target ID:	12
Start time:	05:30:50
Start date:	24/11/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6044 -s 276
Imagebase:	0x7ff679980000
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	7FFC119E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BBF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BBF.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_738eef979a666465c6051ddd5fef4b7e70c91a_4f0e5919_15905d59	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_738eef979a666465c6051ddd5fef4b7e70c91a_4f0e5919_15905d59\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BBF.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BBF.tmp.xml	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6605.tmp.csv	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER66F0.tmp.txt	success or wait	1	7FFC119DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 1d 72 7f 63 fd 05 12 00 00 00 00 00	MDMP rc	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	4924	6	00 00 00 00 00 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	212	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 3c 13 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 fd 1f fd 01 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 fd 71 7f 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 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00	UB<LwTqc0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	5594	1232	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 fd fd 73 72 00 00 00 fd fd fd 73 72 00 00 00 fd fd fd 73 72 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 73 72 00 00 00 30 fd fd 73 72 00 00 00 00 00 05 32 fd 7f 00 00 20 fd 0d 32 fd 7f 00 00 fd 0d 32 fd 7f 00 00 70 fd fd 73 72 00 00 00 50 fd fd 73 72 00 00 00 fd fd fd 73 72 00 00 00 2f fd 0d 32 fd 7f 00	3++S++FHsrsrsrsr0sr2 22psrPsrsr/2	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	1632	168	fd 17 00 00 00 00 00 00 09 04 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 2f fd 0d 32 fd 7f 00 00 01 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 fd 15 00 00	/2	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	8058	20	05 00 00 00 fd fd fd fd fd 01 00 00 08 00 00 00 fd 1f 00 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	8142	8	70 fd 1a 32 fd 7f 00 00	p2	success or wait	4	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	18758	8192	00 00 00 00 00 00 00 00 00 00 fd 73 72 00 00 00 00 40 fd 73 72 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 fd fd 73 72 00 00 00 00 00 00 00 00 00 00 00 fd 17 00 00 00 00 00 00 fd 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 29 fd fd fd 01 00 00 00 fd fd 73 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	sr@srsr)sr	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	1800	4	01 00 00 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	6826	1232	fd fd fd 73 72 00 00 00 20 00 00 00 00 00 00 00 fd 5a 08 32 fd 7f 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 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 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 fd fd 73 72 00 00 00 fd fd fd 73 72 00 00 00 fd fd fd 73 72 00 00 00 00 00 00 00 00 00 00 00 fd fd fd 73 72 00 00 00 30 fd fd 73 72 00 00 00 00 00 05 32 fd 7f 00 00 20 fd 0d 32 fd 7f 00 00 fd 0d 32 fd 7f 00 00 70 fd fd 73 72 00 00 00 50 fd fd 73 72 00 00 00 fd fd fd 73 72 00 00 00 2f fd 0d 32 fd 7f 00	sr Z2 3++S++FHsrsrsrsr0sr2 22psrPsrsr/2	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	1804	48	fd 17 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 73 72 00 00 00 48 fd fd 73 72 00 00 00 fd 20 00 00 fd 20 00 00 fd 04 00 00 fd 1a 00 00	srHsr	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	1864	4	16 00 00 00		success or wait	22	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	4930	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	22	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	4136	120	00 00 fd 2c fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b fd 15 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 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 00 0c 00 00 00 18 00 00 00 01 00 00 00	,<2|h+BB?#`A	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	5560	34	1c 00 00 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 00 00	pzG0rkIchr.dll	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	4256	668	00 00 0e 13 fd 7f 00 00 00 fd 04 00 fd 1c 05 00 fd 2d fd 62 fd 15 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 fd fd 02 00 00 00 00 00 30 fd 02 00 00 00 00 41 37 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4f 69 03 00 00 00 00 00 fd 6c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 36 1b 00 00 00 00 00 4f fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 75 07 05 00 00 00 00 00 1c 7d 76 59 00 00 00 00 45 04 54 16 00 00 00 00 1d fd fd 0f 00 00 00 00 3f 3f 66 01 00 00 00 00 fd fd 00 00 49 fd 00 00 04 fd 05 00 5c fd 0a 00 4f fd 04 00 06 fd 1f 00 75 07 05 00 3d 24 3e 00 fd 16 01 00 fd fd 13 00 00 00 00 00 fd 2b 2c 00 fd 3a 04	-bZb0A7Oil6O@u}vYET??fl\Ou=$>+,:	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	26950	4520	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDC43.tmp.dmp	32	120	03 00 00 00 34 00 00 00 08 07 00 00 04 00 00 00 4c 09 00 00 48 07 00 00 0e 00 00 00 24 00 00 00 fd 10 00 00 05 00 00 00 54 00 00 00 7a 1f 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 28 0b 00 00 fd 6f 00 00 15 00 00 00 fd 01 00 00 fd 10 00 00 16 00 00 00 fd 00 00 00 fd 12 00 00	4LH$Tz`8T(o	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 34 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6044</Pid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 35 00 35 00 36 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>35568</Uptime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 34 00 35 00 39 00 35 00 32 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>2203404595200</VirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 35 00 35 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>1559</PageFaultCount>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 35 00 38 00 37 00 37 00 37 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>5877760</PeakWorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1806	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1810	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 35 00 38 00 37 00 37 00 37 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>5877760</WorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1896	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	1900	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2020	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2024	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 30 00 32 00 38 00 38 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>100288</QuotaPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2128	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2132	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 35 00 34 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>15464</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2262	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2266	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 35 00 33 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>15328</QuotaNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2380	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2384	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 32 00 39 00 30 00 32 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1290240</PagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2466	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2470	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 35 00 35 00 37 00 37 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>1355776</PeakPagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2568	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2572	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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 32 00 39 00 30 00 32 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1290240</PrivateUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2650	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2654	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2704	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2708	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2742	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2746	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2792	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2796	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2804	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1556</Pid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2834	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2838	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2846	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	2930	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3032	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 33 00 39 00 33 00 36 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>39363</Uptime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3088	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3166	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3170	2	09 00		success or wait	4	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3178	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3230	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3234	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3242	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3286	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3290	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3300	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3404	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3478	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3482	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3492	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 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>682</PageFaultCount>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3564	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3568	2	09 00		success or wait	5	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3578	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 38 00 30 00 38 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>2478080</PeakWorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3674	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3678	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3688	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 38 00 30 00 38 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2478080</WorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3768	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3772	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3782	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 37 00 33 00 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>73744</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3894	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3898	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	3908	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 36 00 34 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>66416</QuotaPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4004	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4008	2	09 00		success or wait	5	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4018	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4140	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4144	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4154	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4260	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4264	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4274	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 34 00 37 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>544768</PagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4348	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4352	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4362	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 34 00 37 00 36 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>544768</PeakPagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4452	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4456	2	09 00		success or wait	5	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4466	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 34 00 37 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>544768</PrivateUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4536	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4540	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4548	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4594	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4598	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4604	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4646	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4650	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4654	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4686	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4690	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4692	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4734	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4738	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4740	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4778	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4782	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4786	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 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>BEX64</EventType>	success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4842	4	0d 00 0a 00		success or wait	9	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4846	2	09 00		success or wait	18	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	4850	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	9	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	5596	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	5600	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	5602	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	5642	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	5646	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	5648	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	5686	4	0d 00 0a 00		success or wait	6	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	5690	2	09 00		success or wait	12	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	5694	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6248	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6252	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6254	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6300	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6338	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6342	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6346	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6440	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6444	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6448	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 75 00 64 00 76 00 67 00 75 00 64 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>udvgud, Inc.</SystemManufacturer>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6554	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6558	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6562	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 75 00 64 00 76 00 67 00 75 00 64 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>udvgud7,1</SystemProductName>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6658	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6662	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6666	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6786	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6790	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6794	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 33 00 32 00 35 00 32 00 33 00 38 00 32 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>1623252382</OSInstallDate>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6876	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6880	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6884	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6986	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6990	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	6994	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7062	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7066	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7068	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7114	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7148	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7152	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7156	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7252	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7256	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7258	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7294	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7298	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7300	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7324	4	0d 00 0a 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7328	2	09 00		success or wait	6	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7332	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 38 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>80000000</Flags>	success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7584	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7588	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7590	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7616	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7620	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7622	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 31 00 33 00 3a 00 33 00 31 00 3a 00 31 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-24T13:31:10Z">	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7722	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7726	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7730	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 38 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 30 00 34 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 36 00 34 00 30 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 36 00 34 00 30 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="287" PID="6044" UptimeMS="2640" TimeSinceCreationMS="2640" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7992	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	7996	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8002	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 35 00 33 00 37 00 33 00 39 00 35 00 32 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 30 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5373952" TimelineUnitShift="12" Timeline="10011"/>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8188	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8192	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8196	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8216	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8220	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8222	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8260	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8264	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8266	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8312	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 39 00 65 00 36 00 63 00 37 00 33 00 38 00 2d 00 62 00 66 00 66 00 37 00 2d 00 34 00 62 00 36 00 38 00 2d 00 62 00 37 00 65 00 61 00 2d 00 30 00 64 00 35 00 30 00 35 00 64 00 39 00 35 00 37 00 39 00 34 00 64 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>b9e6c738-bff7-4b68-b7ea-0d505d95794d</Guid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8410	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8414	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8418	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 31 00 33 00 3a 00 33 00 31 00 3a 00 31 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-11-24T13:31:10Z</CreationTime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8516	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8520	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8522	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8562	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER148A.tmp.WERInternalMetadata.xml	8566	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1BBF.tmp.xml	0	4852	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_738eef979a666465c6051ddd5fef4b7e70c91a_4f0e5919_15905d59\Report.wer	0	2	fd fd		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_738eef979a666465c6051ddd5fef4b7e70c91a_4f0e5919_15905d59\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	149	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_738eef979a666465c6051ddd5fef4b7e70c91a_4f0e5919_15905d59\Report.wer	9232	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 31 00 32 00 34 00 31 00 35 00 36 00 37 00 36 00 30 00	MetadataHash=1124156760	success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC119DE3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	FileId	unicode	00002f34ccfdd8141aeee2e89ffb070ce239c7d00706	success or wait	1	7FFC11A01D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LowerCaseLongPath	unicode	c:\windows\system32\rundll32.exe	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LongPathHash	unicode	rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Name	unicode	rundll32.exe	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Publisher	unicode	microsoft corporation	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinFileVersion	unicode	10.0.17134.1	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinaryType	unicode	pe64_amd64	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LinkDate	unicode	05/20/2093 18:03:41	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Size	B	00 10 01 00 00 00 00 00	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Language	dword	1033	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsPeFile	dword	1	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsOsComponent	dword	1	success or wait	1	7FFC11A01D2D	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 AF DE FC 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 00 00 00 00 00 00 00 00	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 2F AA 0D 32 FC 7F 00 00 01 00 00 00 00 00 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FFC11A007CB	RegSetValueExW

Analysis Process: WerFault.exe PID: **5404**, Parent PID: **6136**

General

Target ID:	13
Start time:	05:30:50
Start date:	24/11/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6136 -s 304
Imagebase:	0x7ff679980000
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	7FFC119E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD021.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD021.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_206411b7d18c8b51ef308e99261d801f59953bc0_4f0e5919_15ebd55f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_206411b7d18c8b51ef308e99261d801f59953bc0_4f0e5919_15ebd55f\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC119DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD021.tmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD021.tmp.xml	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC28.tmp.csv	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAC48.tmp.txt	success or wait	1	7FFC119DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 31 72 7f 63 fd 05 12 00 00 00 00 00	MDMP 1rc	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	5080	6	00 00 00 00 00 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.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 00 18 01 8f fd 01 00 00 54 05 00 00 fd 03 00 00 fd 17 00 00 00 72 7f 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 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00	UBLwTrc0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	5750	1232	00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 40 14 fd 2c fd 7f 00 00 fd 78 fd 6b 7a 02 00 00 7d 45 fd 2f fd 7f 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 00 0a 14 06 00 00 00 00 00 70 02 06 00 00 00 00 00 fd fd 4f 70 00 00 00 00 00 0a 00 00 00 00 00 00 00 fd fd 4f 70 fd 00 00 00 3c 0b 50 70 00 00 00 00 2e 4c fd 6b 00 00 00 00 5e fd 4f 70 00 00 00 00 fd 53 fd 6b 00 00 00 00 0a 00 00 00 00 00 00 00 fd fd 61 fd fd 0f 00 00 28 fd 4f 70 fd 00 00 00 6f 53 fd 6b 00 00 00 00 fd fd 4f 70 00 00 00 00 6d fd 05 00 00 00 00 00 49 12 00 00 00 00 00 00 fd 7c 0f 13 fd 7f 00	@,xkz}E/_3++S++pOpOp<Pp.Lk^OpSka(OpoSkOpml|	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	1620	168	fd 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 7c 0f 13 fd 7f 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	10678	20	10 00 00 00 08 fd 57 70 fd 00 00 00 fd 0a 00 00 fd 2a 00 00	Wp*	success or wait	16	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	10938	2808	76 fd 06 32 fd 7f 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 10 00 00 00 00 00 00 00 48 fd 57 70 fd 00 00 00 41 fd 57 70 fd 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 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 7e 70 fd 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 42 fd 6b 7a 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 fd 2f fd 6b 7a 02 00 00 fd fd fd fd fd fd fd 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	v2HWpAWp~pBkz/kzPP	success or wait	15	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	51706	256	6b 10 49 fd 73 18 57 41 54 41 55 41 56 41 57 48 fd fd 60 fd fd 24 fd 00 00 00 44 fd fd fd fd fd fd fd 24 fd 00 00 00 45 fd fd fd 00 00 00 44 fd fd 24 fd 00 00 00 41 fd fd fd 32 00 00 fd fd 24 fd 00 00 00 fd fd fd fd fd fd fd fd fd 0e 00 00 41 fd fd 49 12 00 00 fd fd fd fd fd fd 44 fd fd 4e fd fd fd 41 fd fd 52 01 00 00 49 fd fd 3b fd 0f fd fd 02 00 00 44 3b fd 0f fd 7b 02 00 00 49 fd fd fd 02 00 00 00 0f fd 67 01 00 00 49 fd 09 49 fd fd fd 00 00 00 48 2d 59 3a 00 00 48 01 fd fd 01 00 00 49 fd fd fd 02 00 00 49 fd 01 48 fd fd 49 fd 41 48 fd fd 4e 08 4d fd 4b 48 48 fd fd 28 03 00 00 44 fd fd 30 01 00 00 41 fd fd fd 23 00 00 fd fd fd 01 00 00 fd fd 75 25 48 fd 03 fd fd fd 01 00 00 fd fd 59 02 00 00 fd fd fd 35 00 00 72 0e 48 fd fd fd 01 00 00 48 31 fd fd	kIsWATAUAVAWH`DED$A2$AIDNARI;D;{IgIIH-Y:HIIHIAHNMKHH(D0A#u%HY5rHH1	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	1788	4	03 00 00 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	6982	1232	fd fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 4f 70 fd 00 00 00 fd fd fd fd fd fd fd fd fd 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 fd fd 4f 70 fd 00 00 00 fd fd fd fd fd fd fd fd fd 4f 70 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 fd 4f 70 fd 00 00 00 fd fd 4f 70 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 fd fd 4f 70 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 0e 32 fd 7f 00	Op3++S++FOpOpOpOpOp2	success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	1888	48	0c 14 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 7e 70 fd 00 00 00 fd fd 5f 70 fd 00 00 00 18 0b 00 00 fd 37 00 00 fd 04 00 00 fd 24 00 00	P~p_p7$	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	1948	4	17 00 00 00		success or wait	23	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	4328	752	00 00 fd 2c 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 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 20 fd 02 00 00 00 00 00 20 fd 02 00 00 00 00 45 38 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 51 76 03 00 00 00 00 00 fd 76 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 4e 1b 00 00 00 00 00 08 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 75 07 05 00 00 00 00	,<2|h+\BB?#`AZb E8Qvv8N@u	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.tmp.dmp	51962	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 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCC66.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 46 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	)T8TFT@	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6136</Pid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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 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>000 00000</Cm dLineSignature>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 34 00 39 00 39 00 38 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>49987</Uptime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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>220340565 6064</VirtualSize>	success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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 32 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>1624</PageFaultCount>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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 37 00 35 00 30 00 37 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>6275072</PeakWorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1806	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1810	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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 37 00 35 00 30 00 37 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>6275072</WorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1896	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	1900	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2020	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2024	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2128	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2132	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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 30 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 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>17600</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2262	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2266	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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 30 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>16064</QuotaNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2380	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2384	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2466	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2470	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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>13 63968</Pe akPagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2568	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2572	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2650	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2654	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2704	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2708	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2742	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2746	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2792	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2796	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2804	30	3c 00 50 00 69 00 64 00 3e 00 31 00 35 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1556</Pid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2834	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2838	2	09 00		success or wait	4	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2846	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2918	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2922	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	2930	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3020	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3024	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3032	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 39 00 31 00 38 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>59188</Uptime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3076	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3080	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3088	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3166	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3170	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3178	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3230	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3234	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3242	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3286	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3290	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3300	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 35 00 31 00 33 00 36 00 35 00 31 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4351365120</PeakVirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3404	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 35 00 31 00 33 00 36 00 35 00 31 00 32 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>4351365120</VirtualSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3478	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3482	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3492	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 35 00 30 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>1504</PageFaultCount>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3566	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3570	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3580	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 35 00 31 00 39 00 37 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5197824</PeakWorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3676	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3680	2	09 00		success or wait	5	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3690	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 35 00 31 00 39 00 37 00 38 00 32 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>5197824</WorkingSetSize>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3770	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3774	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3784	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 37 00 39 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 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>79072</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3896	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3900	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	3910	96	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 37 00 38 00 38 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 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>78896</QuotaPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4006	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4010	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4020	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 32 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>5224</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4142	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4146	2	09 00		success or wait	5	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4156	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 35 00 32 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5224</QuotaNonPagedPoolUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4262	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4266	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4276	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 37 00 31 00 36 00 32 00 32 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>1716224</PagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4352	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4356	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4366	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 37 00 31 00 36 00 32 00 32 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>1716224</PeakPagefileUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4458	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4462	2	09 00		success or wait	5	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4472	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 37 00 31 00 36 00 32 00 32 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>1716224</PrivateUsage>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4544	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4548	2	09 00		success or wait	4	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4556	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4602	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4606	2	09 00		success or wait	3	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4612	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4654	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4658	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4662	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4694	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4698	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4700	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4742	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4746	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4748	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4786	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4790	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4794	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4856	4	0d 00 0a 00		success or wait	8	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4860	2	09 00		success or wait	16	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	4864	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	5520	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	5524	2	09 00		success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	5526	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	5566	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	5570	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	5572	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	5610	4	0d 00 0a 00		success or wait	6	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	5614	2	09 00		success or wait	12	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	5618	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6172	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6176	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6178	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6218	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6222	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6224	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6262	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6266	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6270	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6364	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6368	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6372	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 75 00 64 00 76 00 67 00 75 00 64 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>udvgud, Inc.</SystemManufacturer>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6478	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6482	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6486	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 75 00 64 00 76 00 67 00 75 00 64 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>udvgud7,1</SystemProductName>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6582	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6586	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6590	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6710	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6714	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6718	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 33 00 32 00 35 00 32 00 33 00 38 00 32 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>1623252382</OSInstallDate>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6800	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6804	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6808	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6910	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6914	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6918	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6986	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6990	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	6992	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7032	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7036	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7038	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7072	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7076	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7080	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7176	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7180	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7182	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7218	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7222	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7224	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7248	4	0d 00 0a 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7252	2	09 00		success or wait	6	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7256	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7510	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7514	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7516	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7542	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7546	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7548	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 31 00 33 00 3a 00 33 00 31 00 3a 00 33 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-11-24T13:31:30Z">	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7648	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7652	2	09 00		success or wait	2	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7656	258	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 38 00 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 31 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 35 00 36 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 36 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 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 00 31 00 22	<Process AsId="289" PID="6136" UptimeMS="562" TimeSinceCreationMS="562" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1"	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7914	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7918	2	09 00		success or wait	3	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	7924	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 36 00 31 00 30 00 31 00 33 00 37 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 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="16101376" TimelineUnitShift="12" Timeline="1111"/>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8110	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8114	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8118	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8138	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8142	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8144	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8182	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8186	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8188	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8226	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8230	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8234	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 34 00 35 00 61 00 37 00 63 00 38 00 65 00 2d 00 63 00 65 00 66 00 33 00 2d 00 34 00 64 00 64 00 61 00 2d 00 39 00 65 00 62 00 35 00 2d 00 33 00 31 00 35 00 36 00 34 00 61 00 66 00 32 00 65 00 63 00 35 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>545a7c8e-cef3-4dda-9eb5-31564af2ec5c</Guid>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8332	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8336	2	09 00		success or wait	2	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8340	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 31 00 33 00 3a 00 33 00 31 00 3a 00 33 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-11-24T13:31:30Z</CreationTime>	success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8438	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8442	2	09 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8444	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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8484	4	0d 00 0a 00		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF55.tmp.WERInternalMetadata.xml	8488	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	7FFC119DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD021.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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_206411b7d18c8b51ef308e99261d801f59953bc0_4f0e5919_15ebd55f\Report.wer	0	2	fd fd		success or wait	1	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_206411b7d18c8b51ef308e99261d801f59953bc0_4f0e5919_15ebd55f\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	7FFC119DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_pzG_206411b7d18c8b51ef308e99261d801f59953bc0_4f0e5919_15ebd55f\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 32 00 38 00 39 00 32 00 35 00 39 00 38 00 38 00 30 00	MetadataHash=-289259880	success or wait	1	7FFC119DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC11A01D2D	unknown
\REGISTRY\A\{5a15be30-4994-9ade-150c-a3ec62400022}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC119DE3FE	unknown

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	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 2F AA 0D 32 FC 7F 00 00 01 00 00 00 00 00 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 A9 7C 0F 13 FC 7F 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FFC11A007CB	RegSetValueExW

Analysis Process: WerFault.exe PID: **680**, Parent PID: **6136**

General

Target ID:	14
Start time:	05:31:19
Start date:	24/11/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6136 -s 304
Imagebase:	0x7ff679980000
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