ID: 631905
Sample Name: JtJ50Swtfo
Cookbook: default.jbs
Time: 22:27:59
Date: 22/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

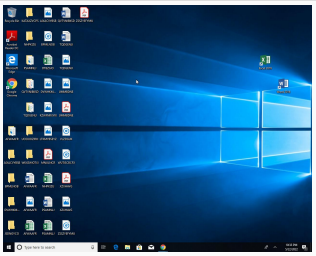
Windows Analysis Report

JtJ50Swtfo

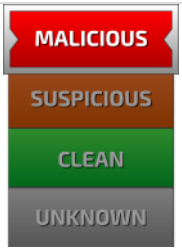
Overview

General Information

Sample Name:	JtJ50Swtfo (renamed file extension from none to dll)
Analysis ID:	631905
MD5:	646ca94d40f268..
SHA1:	22e67eb4d6e4b5.
SHA256:	52769f52f479f16..
Tags:	exe trojan
Infos:	



Detection



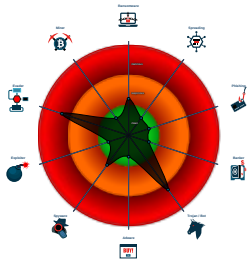
Emotet

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Machine Learning detection for sam…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7096 cmdline: loaddll64.exe "C:\Users\user\Desktop\JtJ50Swtfo.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7104 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\JtJ50Swtfo.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7124 cmdline: rundll32.exe "C:\Users\user\Desktop\JtJ50Swtfo.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 5944 cmdline: C:\Windows\system32\WerFault.exe -u -p 7124 -s 336 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - regsvr32.exe (PID: 7112 cmdline: regsvr32.exe /s C:\Users\user\Desktop\JtJ50Swtfo.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6316 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\GJzmbimn\geJzufDvqRClHij.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 7136 cmdline: rundll32.exe C:\Users\user\Desktop\JtJ50Swtfo.dll,AddIn_FileTime MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 5900 cmdline: C:\Windows\system32\WerFault.exe -u -p 7136 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 3552 cmdline: rundll32.exe C:\Users\user\Desktop\JtJ50Swtfo.dll,AddIn_SystemTime MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 5436 cmdline: C:\Windows\system32\WerFault.exe -u -p 3552 -s 332 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - WerFault.exe (PID: 5148 cmdline: C:\Windows\system32\WerFault.exe -u -p 3552 -s 332 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 6320 cmdline: rundll32.exe C:\Users\user\Desktop\JtJ50Swtfo.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 5788 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3008 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4176 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5328 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6288 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6908 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.458651717.0000000002A20000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000000.461474320.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.495781137.0000018014000000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000000.461684776.00000297062B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000000.470298484.00000297062B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.21310570000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.21310570000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.21310570000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.21310570000.2.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.0.rundll32.exe.297062b0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 17 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

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

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

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

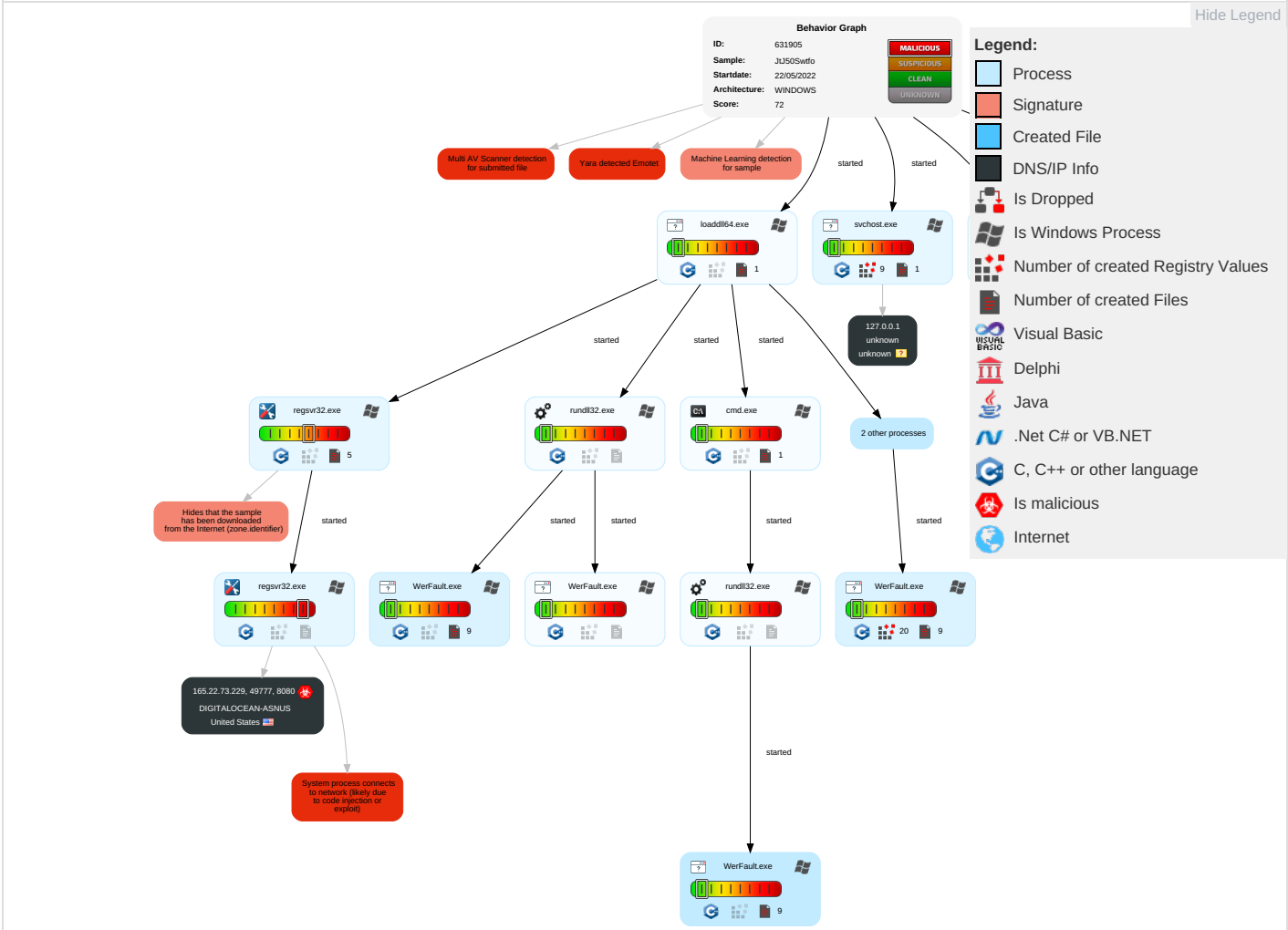
Stealing of Sensitive Information

Yara detected Emotet

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	2 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 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	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Virtualization/Sandbox Evasion	Security Account Manager	4 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	3 Virtualization/Sandbox Evasion	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 Deobfuscate/Decode Files or Information	LSA Secrets	2 Process 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 Hidden Files and Directories	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Regsvr32	Proc Filesystem	2 5 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Rundll32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 DLL Side-Loading	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 File Deletion	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

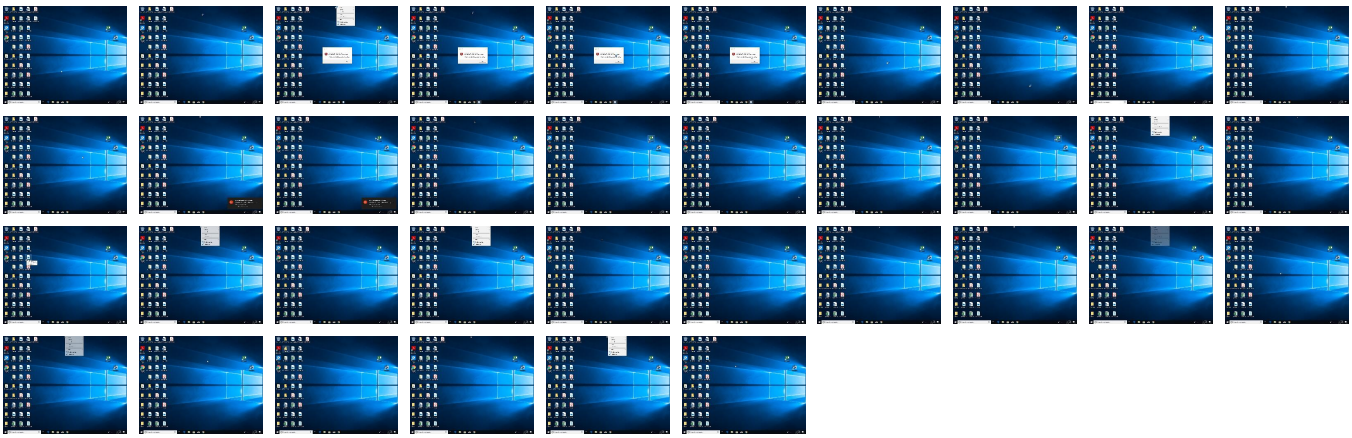
Behavior Graph



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
JtJ50Swtfo.dll	59%	ReversingLabs	Win64.Trojan.Emotet	
JtJ50Swtfo.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.rundll32.exe.21310570000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.18014000000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.21310570000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.18014000000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.18014000000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.2a20000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.0.rundll32.exe.297062b0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.0.rundll32.exe.297062b0000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.0.rundll32.exe.21310570000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.1490000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.rundll32.exe.297062b0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/d	0%	Avira URL Cloud	safe	
http://https://165.22.73.229:8080/	0%	Avira URL Cloud	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://schemas.xmlsoap.o	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://165.22.73.229/	0%	Avira URL Cloud	safe	
http://https://165.22.73.229:8080/z	0%	Avira URL Cloud	safe	
http://https://165.22.73.229:8080/Num	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

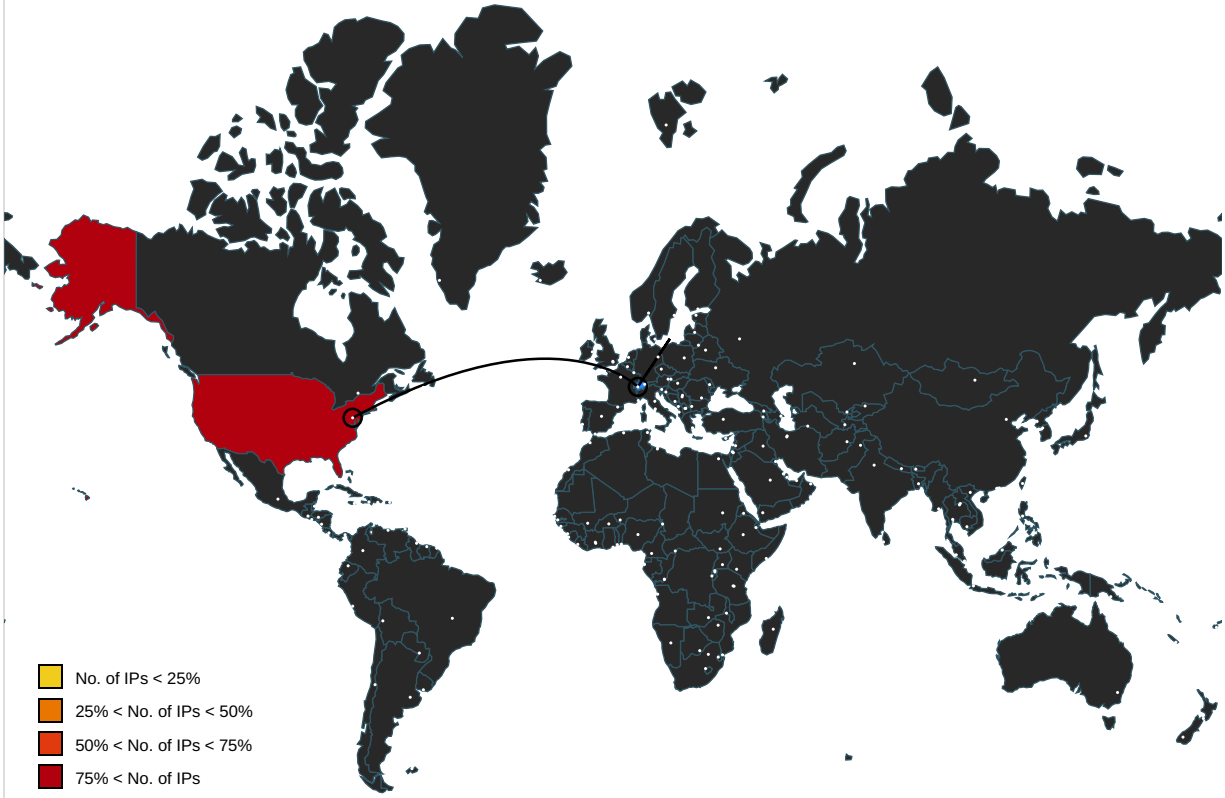
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001C.00000003.824985746.000001E5F2FAF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.824896680.000001E5F2F9E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001C.00000003.824985746.000001E5F2FAF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.824896680.000001E5F2F9E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/d	regsvr32.exe, 00000008.00000002.964035767.00000000012EA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229:8080/	regsvr32.exe, 00000008.00000002.964047666.00000000012F2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.964035767.00000000012EA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001C.00000003.819966685.000001E5F3402000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.820019247.000001E5F2F8D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819907811.000001E5F2FAF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819952245.000001E5F341A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819811916.000001E5F2F9E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819800192.000001E5F2F8D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819925695.000001E5F341A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000001C.00000003.819966685.000001E5F3402000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.820019247.000001E5F2F8D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819907811.000001E5F2FAF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819952245.000001E5F341A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819811916.000001E5F2F9E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819800192.000001E5F2F8D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819925695.000001E5F341A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.o	svchost.exe, 00000010.00000002.847350178.000002136D2AA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.846896392.000002136D2A8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001C.00000003.824985746.000001E5F2FAF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.824896680.000001E5F2F9E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229/	regsvr32.exe, 00000008.00000002.964035767.00000000012EA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229:8080/z	regsvr32.exe, 00000008.00000002.963976122.00000000012B8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229:8080/Num	regsvr32.exe, 00000008.00000003.530907736.00000000012F2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.964047666.00000000012F2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ver)	svchost.exe, 00000010.00000002.847475290.0000021372813000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000002.851676211.000001E5F2F00000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001C.00000003.830088263.000001E5F2F8F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.830129017.000001E5F2FA0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.830206867.000001E5F2FB1000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.830274121.000001E5F3418000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.830231188.000001E5F3418000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 0000001C.00000003.824985746.000001E5F2FAF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.824896680.000001E5F2F9E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 0000001C.00000003.819966685.000001E5F3402000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.820019247.000001E5F2F8D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819907811.000001E5F2FAF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819952245.000001E5F341A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819811916.000001E5F2F9E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819800192.000001E5F2F8D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.819925695.000001E5F341A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
165.22.73.229	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	631905
Start date and time: 22/05/202222:27:59	2022-05-22 22:27:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 33s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	JtJ50Swtfo (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winDLL@27/17@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 73% (good quality ratio 38.9%) • Quality average: 32.7% • Quality standard deviation: 37.6%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 20.189.173.22, 20.42.73.29, 69.192.160.56, 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, onedsblobprdwus17.westus.cloudapp.azure.com, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, onedsblobprdeus15.eastus.cloudapp.azure.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: JtJ50Swtfo.dll

Simulations

Behavior and APIs

Time	Type	Description
22:29:42	API Interceptor	3x Sleep call for process: WerFault.exe modified
22:29:43	API Interceptor	11x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.chk

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.3593198815979092
Encrypted:	false
SSDEEP:	12:SnaaD0JcaaD0JwQQU2naaD0JcaaD0JwQQU:4tgJctgJw/tgJctgJw
MD5:	BF1DC7D5D8DAD7478F426DF8B3F8BAA6
SHA1:	C6B0BDE788F553F865D65F773D8F6A3546887E42
SHA-256:	BE47C764C38CA7A90A345BE183F5261E89B98743B5E35989E9A8BE0DA498C0F2
SHA-512:	00F2412AA04E09EA19A8315D80BE66D2727C713FC0F5AE6A9334BABA539817F568A98CA3A45B2673282BDD325B8B0E2840A393A4DCFADCB16473F5EAF2AF318 0
Malicious:	false
Preview:	.....*.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....*..... ....

C:\ProgramData\Microsoft\Network\Downloader\edb.log

Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24944714559392273
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU44:BJiRdwfu2SRU44
MD5:	3E2858CB05A9D748F750D8039601AB23
SHA1:	55D4E5A52F95F129696CF737D4F32A1C34C09909
SHA-256:	9E2E8BC9DE84ED75E0ACFD61FD791887A08327F0B9174482F5AC9CADFCE86D21
SHA-512:	2C244429562908B15A2186B1477AB7CA158D4EE9A60D55B1B674C0DFB1F527F67A5AD5876E6B174361405EE15675BE7A5E01C61B1FCEEAA631097AD5451AFDF 7
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....d#..... ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x292d39b8, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432

Entropy (8bit):	0.2507046524094365
Encrypted:	false
SSDEEP:	384:8vB+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:8vqSB2nSB2RSjlK/+mLesOj1J2
MD5:	17C3F78317E76B2C2DD76253E2873D75
SHA1:	B19DEF2289166100899C754D126CE94036ED59D0
SHA-256:	F66049E69E4C11374790B7BCBB5F439970EE0BB22478B0C8DA79D7C47A8F6346
SHA-512:	CF93D742329BE22FA8C6C9E0CDC6C48AED0144343E1659CD13AFAA6E40A7C01BAE34AACF1EE37A2F600F96F57464869F939FFFCB3D0192A57B90EFA5DEF3D 6ED
Malicious:	false
Preview:	)-9.... ....e.f.3...w........................).....7 ...z..+....z..h.(.....7 ...z....).............3...w..B...........@............. ....'..7 ...z......................7 ...z.. ....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07485229205221174
Encrypted:	false
SSDEEP:	3:uSlr7vO6z4lAgyatKkS+ll/lle12Vlall3Vkttlmlnl:LlrrO6z4GgyatKkS2llrVA3
MD5:	2B39CA08FECEFC1515366C71F597E30D
SHA1:	2DC245390ADFECB8C661CF7FC83D657B951E377B
SHA-256:	18D6F0A2BFF9DA25FBE25FACF5F73C14722481914BA28A314C073AD82AD1E1CA
SHA-512:	10166219A1E70EFA4592BD4A478237E3A807DEF7E2DDA727215E8E9A9DC7ECFBA897B75CE4A2AA55534DD2E7DC8AF9358BC8B4DEC2BEF34837DA65B47C83D 19D
Malicious:	false
Preview:	.5^......................................3...w..+....z..7 ...z..........7 ...z..7 ...z...F..7 ...z.i....................7 ...z... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_15e02ae a\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7853108972243561
Encrypted:	false
SSDEEP:	96:GWFGspicAJPnyYj455oo7Rl6tpXIQcQPc6cWcEXcw3ufXaXz+HbHgSQgJPb5IDVw:x8eihJK4HhwW9K3jv9/u7sYS274ltZ
MD5:	ACC827E38E39B150496954207F26CF9F
SHA1:	AEECCE7820CD6B08DAC87E16AB391C4E35BE0876
SHA-256:	19A9590BEAA003E8B1C936F8827090E59B4ED9414C38CA62D08177164A6BFD3F
SHA-512:	40103EBC730DCC5CC13B4C9FE07930821DFBC52CDDBC9065C5960FBBC734490F21A92DC88CC432E7FA2C7B28DDCF8E3588CC35E032148E4925DC8294A523E B0
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.=.1.3.2.9.7.7.5.7.3.8.4.3.0.6.4.8.7.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=. 1.3.2.9.7.7.5.7.3.8.6.9.4.7.1.0.4.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.e.6.9.a.e.b.7.-.0.d.b.a.-.4.a.f.a.-.9.6.e.c.-.8.b.6.7.4.8.a.c.f.8.6.1... ..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.=.7.5.b.7.8.d.b.0.-.d.8.e.7.-.4.b.5.1.-.b.0.9.8.-.5.7.d.7.7.e.f.f.8.f.1.5.....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._.J.t.J.5.0.S.w.t.f.o...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.d.e.0.-.0.0.0.1.-.0.0.1.7.-.0.2.d.c.- .b.4.0.e.6.6.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.0.!.0.0.0.0.2.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\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1747af5 d\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.785376784883369

Encrypted:	false
SSDEEP:	96:5EweF2TpiwJPnyHj455oo7Rl6tpXIQcQPc6cWcEhx6cw3hQXaXz+HbHgSQgJPb5Z:5RekiwJKfHhwWAYjv9/u7sYS274ltZ
MD5:	ED96BDCDAAE1D9424028EF842E615A0F
SHA1:	3BAA92D74A6964C50AF8C2029AA6AEEC85DA26AE
SHA-256:	BD9D3EAFE53E1DC3DE3A7A3D1196096535AA68C82811EA99C6A269E2289FA953
SHA-512:	503A9D7DD3D16A85B8C65535064EB776A258507206328BD0490FC797EA96204665C46A067367EFA817798780AA7A150DDE62EB3B9E13BA0B0FD9048F3FF2A031
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.=.1.3.2.9.7.7.5.7.3.6.9.8.0.6.9.6.8.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.5.7.3.7.9.9.1.6.2.6.0.3.....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.=.1.e.b.9.d.3.2.7.-.c.b.9.d.-.4.6.1.c.-.9.0.8.a.-.c.a.a.e.f.6.0.3.6.6.8.0...
..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.=.d.c.e.0.6.9.5.b.-.0.e.5.2.-.4.c.8.7.-.8.4.6.4.-.7.a.a.b.a.6.4.6.b.f.5.7.....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._.J.t.J.5.0.S.w.t.f.o...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.b.e.0.-.0.0.0.1.-.0.0.1.7.-.0.f.e.6.-.6.0.0.c.6.6.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1773b171\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7842975090540836
Encrypted:	false
SSDEEP:	96:b8xFppiqJPnyOj455oo7Rl6tpXIQcQPc6cWcEhx6cw3hQXaXz+HbHgSQgJPb5IDS:aliqJK+HhwWAYjv9/u7sYS274ltZ
MD5:	CBD5581585A10FC5031E233CD69C170A
SHA1:	01AA4FB42F81295A27AB5D9C7F38466034C86BA0
SHA-256:	D4F180660024F2F240D414266211FD669AC40C9CF4BF165D8B2A72820CBAB36E
SHA-512:	FC6926313ABB573E13AB87928BB1F60FC4E7C248CB1D327D7E0FA1B092A76EE249355144833D21B134142210B8DE55F362E3727AF3586DA064E0FB1FFFA5AC4D
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.=.1.3.2.9.7.7.5.7.3.7.0.1.4.6.8.1.4.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.5.7.3.8.0.7.4.0.5.1.5.0.....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.=.3.8.7.0.1.6.e.a.-.4.7.4.0.-.4.5.9.d.-.8.b.1.5.-.9.c.f.4.2.2.b.6.0.b.b.a...
..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.=.6.e.f.4.e.c.7.b.-.9.e.9.b.-.4.c.9.4.-.8.f.e.7.-.4.e.e.4.2.c.a.f.6.c.4.4.....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._.J.t.J.5.0.S.w.t.f.o...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.b.d.4.-.0.0.0.1.-.0.0.1.7.-.6.c.9.8.-.1.a.0.c.6.6.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 05:29:45 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	66212
Entropy (8bit):	2.280297288692693
Encrypted:	false
SSDEEP:	384:ByO904cSe2YqH2FC/HK7dlwcldYnUxUo88fvrW:cufMqH2FC/qdlw+t88K
MD5:	E2CFC23224F78A477BDF042747F96436
SHA1:	60BE11384E5D6E36A75EE5F189F0F3767B2EF495
SHA-256:	6A08D0241262573BF1098020EC3BD5807B9303C361E801C510A35F49E893EE65
SHA-512:	93105110026D42D7CDD48C2F5C04CA78F59FB6D7434741849CF3F4203536C1F5E4B1719429BB3005ECD45FBD8991690B1431357536C8BBB1D96C7E487F9075F9
Malicious:	false
Preview:	MDMP..... .....b.....8.....$...d;.....`.....8.....T.....".....$.....U.....B.....P%...
...Lw.....|.....T.....b.....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\WER2127.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6678
Entropy (8bit):	3.72760217005663
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiEax6jSooYhNSx8CCpr989b4gW7fVom:RrlsNiJojSooYhNSP4p7fv

MD5:	2F521D7AB8C6ABEE091480261B1BC764
SHA1:	A590641E5DB006BE00B856A417765510EB700AFE
SHA-256:	B9DF3C362BC36875DAC16029D2D9D38057DDDE078DE32AB3160F8FFC63CD150E
SHA-512:	8A7BDF77DEAB242631FCF0B5BB570BF2CDF409E2FFBC2D3C545B7FF1097F922533390AA9B107F2AC5C94B89A410937B5016D9F2D01EC345AA5F51A673FD62A A
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.>.3.5.5. 2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER235A.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4892
Entropy (8bit):	4.505358903748867
Encrypted:	false
SSDEEP:	48:cvIwSD8zsXJgtBI9KcWgc8sqYjf8fm8M4JCRCII+nFEXyq8vhII+m0ZESC5SMd:uITf5AVgrsqYQJtvW3eVvMd
MD5:	13555536D901F4E1034B9843C71A46E9
SHA1:	44FC1A57192C982684C753D56B0BFE4A638C2518
SHA-256:	C415F810072D8F5047AFDBAE7194416794CFB0B258F5B72579792F0B7773FAF1
SHA-512:	0B7A9324415AD89DA811417331151E5A93CD99D051FA9AD24274321A27AADB07B9767380A04A817EEBCC97FA8C465672FBCBEB69180681C80C74EB759CB04CD 1
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="1527280" />.. <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\WER7F45.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 05:29:37 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	65216
Entropy (8bit):	2.2879602329885613
Encrypted:	false
SSDEEP:	384:m04cSe2YqH29QC7FcldYn1QYSXsLvaGRB:mfMqH29QCx+FYSXg
MD5:	5F036A0EE06E7F8A37F2916DACA3FD90
SHA1:	E0BE7693EACEE0FD3004AB408091FCAEFC214100
SHA-256:	23677DE67B59ECDDB4F42D5E4062803F711A0554A2E9244BCB8F5441D040C4D8
SHA-512:	E642656D8470B34B1743E6CBE55997AB278100D2AE9D7A5FD7BB4B6056A8153B3D67086967D2D41F947854F5AB597C210D2F6B7956861DCFCAEBB4C9BE29A90 8
Malicious:	false
Preview:	MDMP..... .....b.....8.....$...d;.....`.....8.....T.....X...h.....".....$.....U.....B.....P%... ...Lw.....D...T.....b.....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\WER809D.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 05:29:38 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64428
Entropy (8bit):	2.3099754861449417
Encrypted:	false
SSDEEP:	384:j04cSe2YqH2nbNCKUDPpcldYnCSG5a6p:jfMqH2bNCKC+tH
MD5:	1DE1EC7CED80A4369CF671C0CCAF96E1
SHA1:	A8892CBE7C9497C66B2736993B3DDE55F359AFB3

SHA-256:	F11BF9E703C8D45A280388947283D9F82AC1152CBF34C6CA747FC23D708C5D39
SHA-512:	0C99F5E4261D6935B152DE77152A4D04C8247B50BF2015A6ADC272359FDD9F448035268E6830566CA8C2AB7721BF856704D8FA78E39C5F5D92829BBEBCCB3AE D
Malicious:	false
Preview:	MDMP..... .....b.....8.....$...d;.....`.....8.....T.....".....$.....U.....B.....P%... ...Lw.....T(o...T.....b.....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\WERA01C.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6664
Entropy (8bit):	3.725950692747971
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimJx/Ul+H3kYhNSxACprJ89bRt/fv7m:RrlsNil5Ul+HUYhNSoRFfK
MD5:	6001D212B5EB3A7ABBF335C898D3C3C5
SHA1:	4894F791110FAEB18D9EC772C9CC4BF86B2FCE75
SHA-256:	CF5603ABB60C16F4560F7AA77322A0CFBD3DFC15F58D94ABD75E9D1802045C35
SHA-512:	5E71DAB490BFD9A5C88C9F5149C1F579678BD14122FBD0E1692D78DBB2C80B3823E087A4BCB1F8196507AC4423EE0DF36E8DF6A1581CBFC157D6CCEBB0E47 B0A
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.>.7.1.3. 6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA33A.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4892
Entropy (8bit):	4.503869739793946
Encrypted:	false
SSDEEP:	48:cvlwSD8zsXJgtBI9KcWgc8sqYj78fm8M4JCRCII+nF7yq8vhII+P0ZESC5Spd:uITf5AVgrsqY8Jt8W3JVvpd
MD5:	47AA0CE1F66ACB829997A6775FD25EB2
SHA1:	2E7B95D962BBF68430388A686744AD4F60412F81
SHA-256:	A65356709DD7AD26A14B1EDA3F53F7FE2E79F9B0A556AB53F0FBA1CB479CE5C5
SHA-512:	5A801063C35EFA6616CB61E9EEA970E4CEA5559AFC9E9A3A72C04DAC8693C8F222CA1FC7CAF7C5940DA4323B27CC9964EFC7AAB0F54C99B92EBDA0E82A3E 8A2B
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="1527280" />.. <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\WERA3F4.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8654
Entropy (8bit):	3.7019577354697155
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNil+TUB+gh6Y8aBDgmfhNSxACpr889blf2fa4m:RrlsNicTUB+gh6YXDgmfhNSHI+f0
MD5:	1750C18A710CBAD9A9B097441376D048
SHA1:	7577D35041786C148A49C98C099B99239208AD7B
SHA-256:	81CC89B90768B2E03E8F4A780AC65E00AA8CA148560FB9A8D4CD1B41E1267785
SHA-512:	3A92B9D8D79013DA61AA48AFBA0D92C6F52B53178C953BFACD04D7FD62270F7581679BDA03580DCFF6770B3072DC62CF10F225FC8426A084449B3A2C3F7D66

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.>.7.1.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7DD.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4892
Entropy (8bit):	4.50421410004922
Encrypted:	false
SSDEEP:	48:cvIwSD8zsXJgtBI9KcWgc8sqYjl8fm8M4JCRCII+nFjyq8vhII+D0ZESC5Smd:uITf5AVgrsqYGJtsW3VVvmd
MD5:	DACBE25C80B0FF301B54B760288687C5
SHA1:	BF0A6F8F31707964EE580656201C96D07AC05322
SHA-256:	C2382A5F6DECE4378F908631D2EFE6208690E1F87E3C2CC5D8F3A6E14A9A1653
SHA-512:	BCD8A4E4B5C4D51EB6643C72ECBED76EEB5F38F90946F5A3626666D1029FE1174328B679DD770C284E2247BD35DE34D773DF6BDE7B1EF71C18032F3AFD0C87E1
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="1527280" />.. <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:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp

Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	7.152718217466625
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:	JtJ50Swtfo.dll
File size:	371200
MD5:	646ca94d40f268c87215ffea9fd0e826
SHA1:	22e67eb4d6e4b5f09e3de5a6021462adcf99fe75
SHA256:	52769f52f479f16d61c449d307c7fd1fa23faa0b5589500e0967cd7955ca93d6
SHA512:	5ae522eb99551146f84f9aa94f270083cedc1bb8df26697e15d57fcf7af126766f8f18ed4ffac06df46d88e07c08a8523cd8a4187af3dd8173baf35272de794b
SSDEEP:	6144:hlNuuXQASByX7LxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7xy/BJ7rGTK/V3

TLSH:	36848E46F7F551E5E8F7C13889A23267F9317C948B38A7CB8A44466A4F70BA0E93D701
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik...k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich..ik.....PE..d....{.b....."

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180003580
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x62877BF5 [Fri May 20 11:31:01 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	ad5c5b0f3e2e211c551f3b5059e614d7

Entrypoint Preview

Instruction
dec esp
mov dword ptr [esp+18h], eax
mov dword ptr [esp+10h], edx
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 28h
cmp dword ptr [esp+38h], 01h
jne 00007F0D9877FCD7h
call 00007F0D98785037h
dec esp
mov eax, dword ptr [esp+40h]
mov edx, dword ptr [esp+38h]
dec eax
mov ecx, dword ptr [esp+30h]
call 00007F0D9877FCE4h
dec eax
add esp, 28h
ret
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
dec esp
mov dword ptr [esp+18h], eax
mov dword ptr [esp+10h], edx
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 48h
mov dword ptr [esp+20h], 00000001h
cmp dword ptr [esp+58h], 00000000h
jne 00007F0D9877FCE2h
cmp dword ptr [00028DE8h], 00000000h
jne 00007F0D9877FCD9h
xor eax, eax
jmp 00007F0D9877FDF4h
cmp dword ptr [esp+58h], 01h
je 00007F0D9877FCD9h
cmp dword ptr [esp+58h], 02h
jne 00007F0D9877FD20h
dec eax
cmp dword ptr [0001ED99h], 00000000h
je 00007F0D9877FCEAh
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call dword ptr [0001ED83h]
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
je 00007F0D9877FCE9h
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call 00007F0D9877FA3Ah
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
jne 00007F0D9877FCD9h
xor eax, eax

Rich Headers

Programming Language:	• [LNK] VS2010 build 30319 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [EXP] VS2010 build 30319 • [RES] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2aab0	0x84	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2a1e4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x30000	0x2e9fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x2f000	0xfcc	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5f000	0x294	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x22000	0x298	.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	0x203fa	0x20400	False	0.405439983043	zlib compressed data	5.75409030586	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x22000	0x8b34	0x8c00	False	0.275446428571	data	4.41532108635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2b000	0x3798	0x1400	False	0.161328125	data	2.21550179132	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x2f000	0xfcc	0x1000	False	0.5048828125	data	5.08183440168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x30000	0x2e9fc	0x2ea00	False	0.887011980563	data	7.85049584102	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5f000	0x6fc	0x800	False	0.21435546875	data	2.34217115221	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_FONTDIR	0x300a0	0x2e800	data	English	United States
RT_MANIFEST	0x5e8a0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetTimeFormatA, GetDateFormatA, GetThreadLocale, FileTimeToSystemTime, VirtualAlloc, ExitProcess, CloseHandle, CreateFileW, SetStdHandle, GetCurrentThreadId, FlsSetValue, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, RtlUnwindEx, EncodePointer, FlsGetValue, FlsAlloc, FlsFree, SetLastError, GetLastError, HeapSize, HeapValidate, IsBadReadPtr, DecodePointer, GetProcAddress, GetModuleHandleW, SetHandleCount, GetStdHandle, InitializeCriticalSectionAndSpinCount, GetFileType, GetStartupInfoW, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapSetInformation, GetVersion, HeapCreate, HeapDestroy, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, EnterCriticalSection, LeaveCriticalSection, GetACP, GetOEMCP, GetCPInfo, IsValidCodePage, HeapAlloc, GetModuleFileNameW, HeapReAlloc, HeapQueryInformation, HeapFree, WriteFile, LoadLibraryW, LCMapStringW, MultiByteToWideChar, GetStringTypeW, OutputDebugStringA, WriteConsoleW, OutputDebugStringW, RaiseException, RtlPcToFileHeader, SetFilePointer, GetConsoleCP, GetConsoleMode, FlushFileBuffers
USER32.dll	MessageBoxA
ole32.dll	CoTaskMemFree, CoTaskMemAlloc, CoLoadLibrary

Exports

Name	Ordinal	Address
AddIn_FileTime	1	0x180001140
AddIn_SystemTime	2	0x1800010b0
DllRegisterServer	3	0x180003110

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	

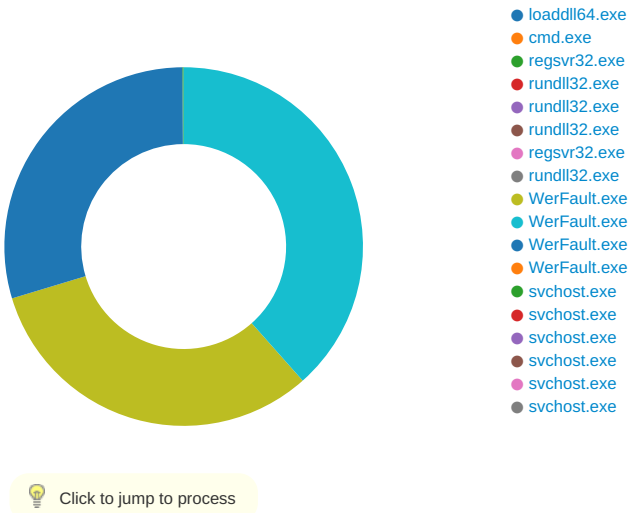
Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 22:29:59.489087105 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:29:59.531128883 CEST	8080	49777	165.22.73.229	192.168.2.5
May 22, 2022 22:29:59.531321049 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:29:59.628360033 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:29:59.670537949 CEST	8080	49777	165.22.73.229	192.168.2.5
May 22, 2022 22:29:59.680217028 CEST	8080	49777	165.22.73.229	192.168.2.5
May 22, 2022 22:29:59.680253983 CEST	8080	49777	165.22.73.229	192.168.2.5
May 22, 2022 22:29:59.680344105 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:30:00.540261030 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:30:00.608218908 CEST	8080	49777	165.22.73.229	192.168.2.5
May 22, 2022 22:30:00.608436108 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:30:00.648366928 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:30:00.732100964 CEST	8080	49777	165.22.73.229	192.168.2.5
May 22, 2022 22:30:00.900325060 CEST	8080	49777	165.22.73.229	192.168.2.5
May 22, 2022 22:30:00.900473118 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:30:03.899759054 CEST	8080	49777	165.22.73.229	192.168.2.5
May 22, 2022 22:30:03.899795055 CEST	8080	49777	165.22.73.229	192.168.2.5
May 22, 2022 22:30:03.899924040 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:30:03.899954081 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:31:49.447776079 CEST	49777	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:31:49.447818995 CEST	49777	8080	192.168.2.5	165.22.73.229

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 7096, Parent PID: 3972

General

Target ID:	0
Start time:	22:29:16
Start date:	22/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\JtJ50Swtfo.dll"
Imagebase:	0x7ff7a0d20000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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: cmd.exe PID: 7104, Parent PID: 7096

General

Target ID:	1
Start time:	22:29:17
Start date:	22/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\JtJ50Swtfo.dll",#1
Imagebase:	0x7ff602050000
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: 7112, Parent PID: 7096

General

Target ID:	2
Start time:	22:29:17
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\JtJ50Swtfo.dll
Imagebase:	0x7ff705580000
File size:	24064 bytes

MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.458651717.0000000002A20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.459283574.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\GJzmbimn\geJzufDvqRClHij.dll:Zone.Identifier	success or wait	1	18002C502	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7124**, Parent PID: **7104**

General

Target ID:	3
Start time:	22:29:17
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\JtJ50Swtfo.dll",#1
Imagebase:	0x7ff7d2730000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.495781137.0000018014000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.454207000.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.454739254.0000018014000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.457838374.0000018014000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.494965359.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.456381918.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **7136**, Parent PID: **7096**

General

Target ID:	4
Start time:	22:29:18
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\JtJ50Swtfo.dll,AddIn_FileTime
Imagebase:	0x7ff7d2730000
File size:	69632 bytes

MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.454696390.0000021310570000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.457901753.0000021310570000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.492879250.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.457423446.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.454349685.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.493226824.0000021310570000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **3552**, Parent PID: **7096**

General

Target ID:	5
Start time:	22:29:22
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\JtJ50Swtfo.dll,AddIn_SystemTime
Imagebase:	0x7ff7d2730000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.461474320.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.461684776.00000297062B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.470298484.00000297062B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.465354445.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.507680225.00000297062B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.507222158.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **6316**, Parent PID: **7112**

General

Target ID:	8
Start time:	22:29:24
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\GJzmbimn\geJzufDvqRClHij.dll"
Imagebase:	0x7ff705580000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.964474360.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.964188108.0000000001490000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6320**, Parent PID: **7096**

General

Target ID:	9
Start time:	22:29:26
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\JtJ50Swtfo.dll,DllRegisterServer
Imagebase:	0x7ff7d2730000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **5900**, Parent PID: **7136**

General

Target ID:	11
Start time:	22:29:27
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 7136 -s 328
Imagebase:	0x7ff76a840000
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	7FFA607F527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA33A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA33A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1747af5d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1747af5d\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA33A.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA33A.tmp.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER74C8.tmp.csv	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER74D8.tmp.txt	success or wait	1	7FFA607EE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 fd 1b fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.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 50 25 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 fd 44 02 00 00 54 05 00 00 fd 03 00 00 fd 1b 00 00 fd 1b fd 62 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 00 02 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 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	UBP%LwDTb0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	10276	1232	00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 73 fd fd 7f 00 00 40 14 23 6e fd 7f 00 00 fd 3b 42 10 13 02 00 00 7d 45 40 71 fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 02 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 fd fd 77 fd fd 6e 00 00 00 00 73 fd fd 7f 00 00 00 00 73 fd fd 7f 00 00 00 00 73 fd fd 7f 00 00 38 fd 15 fd fd 00 00 00 fd fd 15 fd fd 00 00 00 fd 03 03 00 00 00 00 00 08 fd 15 fd fd 00 00 00 6a 5b 41 10 13 02 00 00 0a 00 00 00 00 00 00 00 28 fd 66 4a fd 0f 00 00 fd fd fd fd fd fd fd 00 5b 41 10 13 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 10 42 10 13 02 00 00 fd 00 00 00 00 00 00	s@#n;B}E@q_3++S++wnsss8j[A(fJ[AB	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	1632	168	fd 1b 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	15204	20	52 00 00 00 00 fd 02 fd 01 00 00 00 06 00 00 00 fd 40 00 00	R@	success or wait	82	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	16520	6	01 04 01 00 04 22	"	success or wait	81	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	57092	2888	76 fd 7a 73 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 fd 10 00 00 00 00 00 00 00 fd fd 1d fd fd 00 00 00 fd fd 1d fd 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 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 20 39 fd 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 fd fd fd fd fd fd fd fd 60 43 41 10 13 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 41 10 13 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	vzs 9`CA/APP	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	11508	1232	fd fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 30 fd 15 fd 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 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 38 fd 15 fd fd 00 00 00 fd fd fd fd fd fd fd fd 38 fd 15 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 15 fd 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 fd fd fd fd fd fd 38 fd 15 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 82 73 fd 7f 00	03++S++F888s	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	1900	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 39 fd fd 00 00 00 48 fd 47 fd fd 00 00 00 fd 09 00 00 fd 4a 00 00 fd 04 00 00 fd 36 00 00	p9HGJ6	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	9558	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	25	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	4556	4344	00 00 23 6e fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 0a 28 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 53 01 00 00 04 00 00 00 fd fd 73 fd 7f 00 00 fd fd 73 fd 7f 00 00 00 00 03 fd 01 00 00 00 4c fd fd 0f 66 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 01 00 00 00 00 00	#n<2|h+(BB?#`A pSssLfnS	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	8908	644	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 60 fd 02 00 00 00 00 00 50 fd 02 00 00 00 00 fd 11 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd 03 00 00 00 00 00 50 03 00 00 00 00 00 00 00 00 00 00 00 00 00 70 fd 1a 00 00 00 00 00 fd 2a 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 0a 06 00 00 00 00 00 1e fd fd 00 00 00 00 fd fd fd 1d 00 00 00 00 0b 5f fd 20 00 00 00 00 fd 19 09 01 00 00 00 00 2a 26 01 00 fd fd 00 00 1b fd 05 00 26 fd 0a 00 fd 2a 05 00 06 7f 15 00 fd 0a 06 00 71 02 3a 00 fd fd 01 00 1f 67 15 00 00 00 00 00 55 11 26 00 31 61 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 02 00	Zb`Pp*@_ *&&*q:gU&1a	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	59980	5236	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7F45.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 fd 10 00 00 38 12 00 00 05 00 00 00 24 05 00 00 64 3b 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 58 0d 00 00 68 fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	8$d;`8TXh"$	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7136</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20177</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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 35 00 30 00 33 00 38 00 33 00 37 00 31 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 03837184 </PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.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 38 00 31 00 37 00 31 00 30 00 30 00 38 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>220340817 1008</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1626	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 32 00 39 00 33 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>26293 </PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1712	100	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 31 00 30 00 35 00 30 00 31 00 33 00 32 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>105013248</PeakWorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1822	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 37 00 30 00 34 00 35 00 31 00 32 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>7045120</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	1912	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 36 00 37 00 37 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	<QuotaPeakPagedPoolUsage>106776</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2036	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 36 00 35 00 37 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>106576</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2144	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 32 00 31 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>21600</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2278	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 32 00 31 00 32 00 34 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>21248</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2396	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 38 00 34 00 33 00 32 00 30 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>1843200</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2482	96	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 30 00 31 00 34 00 37 00 34 00 33 00 30 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>101474304</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2588	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 38 00 34 00 33 00 32 00 30 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>1843200</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2668	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2720	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2768	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2806	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2810	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2814	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2870	4	0d 00 0a 00		success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2874	2	09 00		success or wait	18	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	2878	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 4a 00 74 00 4a 00 35 00 30 00 53 00 77 00 74 00 66 00 6f 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_JtJ50Swtfo.dll</Parameter0>	success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	3670	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	3710	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	3714	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	3716	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	3754	4	0d 00 0a 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	3758	2	09 00		success or wait	12	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	3762	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4316	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4320	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4322	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4368	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4406	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4410	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4414	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4516	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 77 00 6b 00 63 00 73 00 71 00 6e 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>wkcsqn, Inc.</SystemManufacturer>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4630	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 77 00 6b 00 63 00 73 00 71 00 6e 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>wkcsqn7,1</SystemProductName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4726	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4730	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4734	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4862	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 30 00 37 00 32 00 34 00 30 00 34 00 39 00 37 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>1607240497</OSInstallDate>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4944	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4948	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	4952	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5054	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5058	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5062	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5130	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5134	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5136	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5176	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5180	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5182	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5216	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5220	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5224	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5320	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5324	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5326	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5362	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5366	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5368	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5392	4	0d 00 0a 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5396	2	09 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5400	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5646	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5650	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5652	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5678	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5682	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5684	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 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 33 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T05:29:38Z">	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5784	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5788	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	5792	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 34 00 31 00 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 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 34 00 39 00 39 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 34 00 39 00 39 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="413" PID="7136" UptimeMS="5499" TimeSinceCreationMS="5499" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6054	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6058	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6064	182	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 34 00 37 00 34 00 33 00 31 00 36 00 38 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 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="4743168" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6246	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6250	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6254	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6274	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6278	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6280	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6318	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6322	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6324	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6362	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6366	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6370	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 65 00 62 00 39 00 64 00 33 00 32 00 37 00 2d 00 63 00 62 00 39 00 64 00 2d 00 34 00 36 00 31 00 63 00 2d 00 39 00 30 00 38 00 61 00 2d 00 63 00 61 00 61 00 65 00 66 00 36 00 30 00 33 00 36 00 36 00 38 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>1eb9d327-cb9d-461c-908a-caaef6036680</Guid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6468	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6472	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6476	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 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 33 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-23T05:29:38Z</CreationTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6574	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6578	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6580	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6620	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA01C.tmp.WERInternalMetadata.xml	6624	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA33A.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1747af5d\Report.wer	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1747af5d\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	152	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1747af5d\Report.wer	9584	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 32 00 31 00 31 00 31 00 31 00 32 00 38 00 32 00 39 00 35 00	MetadataHash=2111128295	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: WerFault.exe PID: **5944**, Parent PID: **7124**

General

Target ID:	12
Start time:	22:29:28
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 7124 -s 336
Imagebase:	0x7ff76a840000
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	7FFA607F527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7DD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7DD.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1773b171	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1773b171\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7DD.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7DD.tmp.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7815.tmp.csv	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER7836.tmp.txt	success or wait	1	7FFA607EE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 1b fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.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 50 25 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 54 28 6f 02 00 00 54 05 00 00 fd 03 00 00 fd 1b 00 00 fd 1b fd 62 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 02 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 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBP%LwT(oTb0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	10276	1232	00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 73 fd fd 7f 00 00 40 14 23 6e fd 7f 00 00 fd 3a fd 13 fd 01 00 00 7d 45 40 71 fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 06 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7b 35 17 fd 7b 6e 00 00 00 00 73 fd fd 7f 00 00 00 00 73 fd fd 7f 00 00 00 00 73 fd fd 7f 00 00 78 fd 4c fd 1f 00 00 00 fd fd 4c fd 1f 00 00 00 fd 03 10 00 00 00 00 00 48 fd 4c fd 1f 00 00 00 16 53 fd 13 fd 01 00 00 0a 00 00 00 00 00 00 00 28 fd 66 4a fd 0f 00 00 fd fd fd fd fd fd fd fd 52 fd 13 fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 11 fd 13 fd 01 00 00 fd 00 00 00 00 00 00	s@#n:}E@q_3++S++ {5{nsssxLLHLS(fJRX	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	1632	168	fd 1b 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	15204	20	52 00 00 00 fd fd 4c fd 1f 00 00 00 08 00 00 00 fd 40 00 00	RL@	success or wait	82	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	16520	8	4f 7e fd 73 fd 7f 00 00	O~s	success or wait	81	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	59076	8	fd fd 5c fd 1f 00 00 00	\	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	11508	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 70 fd 4c fd 1f 00 00 00 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 78 fd 4c fd 1f 00 00 00 fd fd fd fd fd fd fd 78 fd 4c fd 1f 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 4c fd 1f 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 78 fd 4c fd 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 82 73 fd 7f 00	pL3++S++FxLxLLxLs	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	1900	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 7e fd 1f 00 00 00 fd fd 5c fd 1f 00 00 00 58 06 00 00 fd 76 00 00 fd 04 00 00 fd 36 00 00	~\Xv6	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	9558	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	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	4556	4344	00 00 23 6e fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 0a 28 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 53 01 00 00 04 00 00 00 fd fd 73 fd 7f 00 00 fd fd 73 fd 7f 00 00 00 00 03 fd 01 00 00 00 f3 40 0f 66 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 01 00 00 00 00 00	#n<2|h+(BB?#`A pSss@fnS	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	8908	644	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 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 2f 02 00 00 00 00 00 50 fd 02 00 00 00 00 fd 11 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd 03 00 00 00 00 00 50 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7e fd 1a 00 00 00 00 00 fd 2a 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 0a 06 00 00 00 00 00 1e fd fd 00 00 00 00 3c f2 1d 00 00 00 00 fd 74 fd 20 00 00 00 00 7e fd 09 01 00 00 00 00 3e 26 01 00 fd fd 00 00 21 fd 05 00 fd fd 0a 00 fd 2a 05 00 06 7f 15 00 fd 0a 06 00 fd 57 3a 00 20 fd 01 00 fd 7d 15 00 00 00 00 00 1d 55 26 00 5a 61 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 02 00	ZbP~*@<t ~>&!*W: }U&Za	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	59084	5344	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER809D.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 fd 10 00 00 38 12 00 00 05 00 00 00 24 05 00 00 64 3b 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 fd 0d 00 00 04 fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	8$d;`8T"$	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7124</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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>00000000</CmdLineSignature>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 36 00 31 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>21618</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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 35 00 30 00 33 00 38 00 30 00 30 00 33 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>2203503800320 </PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.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 38 00 31 00 37 00 31 00 30 00 30 00 38 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>2203408171008</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1626	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 32 00 39 00 31 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>26291</PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1712	100	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 31 00 30 00 35 00 30 00 31 00 33 00 32 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>105013248</PeakWorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1822	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 37 00 30 00 35 00 33 00 33 00 31 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>7053312</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	1912	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 36 00 37 00 37 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	<QuotaPeakPagedPoolUsage>106776</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2036	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 36 00 35 00 37 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>106576</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2144	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 32 00 31 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21568</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2278	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 32 00 31 00 32 00 31 00 36 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>21216</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2396	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 38 00 33 00 35 00 30 00 30 00 30 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>1835008</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2482	96	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 30 00 31 00 34 00 36 00 36 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101466112</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2588	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 38 00 33 00 35 00 30 00 30 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>18350088</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2668	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2722	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2752	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2756	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2762	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2802	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2806	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2814	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7104</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2844	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2848	2	09 00		success or wait	4	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2856	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2916	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2920	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	2928	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3018	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3022	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3030	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 32 00 30 00 33 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>22030</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3086	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3176	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3240	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3298	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 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 00 38 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>2203370262528</PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3408	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 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 00 38 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>2203370262528</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3502	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 37 00 39 00 31 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>791</PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3588	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 39 00 32 00 30 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2920448</PeakWorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3684	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3688	2	09 00		success or wait	5	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3698	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 38 00 30 00 31 00 36 00 36 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>2801664</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3792	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 32 00 37 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>27840</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	3918	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 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>27664</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4014	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4018	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4028	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 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>4208</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4164	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 36 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>3664</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4284	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 38 00 35 00 39 00 38 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>2985984</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4360	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4364	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4374	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 33 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3133440</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4480	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 38 00 35 00 39 00 38 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>2985984</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4564	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4620	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4670	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4708	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4756	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4802	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4858	4	0d 00 0a 00		success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4862	2	09 00		success or wait	18	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	4866	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 4a 00 74 00 4a 00 35 00 30 00 53 00 77 00 74 00 66 00 6f 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_JtJ50 Swtfo.dll</Parameter0>	success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	5652	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	5656	2	09 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	5658	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	5698	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	5702	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	5704	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	5742	4	0d 00 0a 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	5746	2	09 00		success or wait	12	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	5750	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6304	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6308	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6310	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6350	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6354	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6356	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6402	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6496	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6500	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6504	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 77 00 6b 00 63 00 73 00 71 00 6e 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>wkcsqn, Inc.</SystemManufacturer>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6610	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6614	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6618	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 77 00 6b 00 63 00 73 00 71 00 6e 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>wkcsqn7,1</SystemProductName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6714	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6718	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6722	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6842	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6846	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6850	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 30 00 37 00 32 00 34 00 30 00 34 00 39 00 37 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>1607240497</OSInstallDate>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6932	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6936	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	6940	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7042	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7046	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7050	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7118	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7122	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7124	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7164	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7168	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7170	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7212	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7308	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7312	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7314	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7350	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7354	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7356	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7380	4	0d 00 0a 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7384	2	09 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7388	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7634	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7638	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7640	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7666	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7670	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7672	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 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 33 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T05:29:39Z">	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7772	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7776	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	7780	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 34 00 31 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 31 00 32 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 35 00 34 00 35 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 34 00 35 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 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="412" PID="7124" UptimeMS="5453" TimeSinceCreationMS="5453" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8052	184	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 34 00 37 00 34 00 33 00 31 00 36 00 38 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="4743168" TimelineUnitShift="12" Timeline="1111"/>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8236	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8240	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8244	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8264	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8268	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8270	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8308	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8312	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8314	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8352	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8356	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8360	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 38 00 37 00 30 00 31 00 36 00 65 00 61 00 2d 00 34 00 37 00 34 00 30 00 2d 00 34 00 35 00 39 00 64 00 2d 00 38 00 62 00 31 00 35 00 2d 00 39 00 63 00 66 00 34 00 32 00 32 00 62 00 36 00 30 00 62 00 62 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>387016ea-4740-459d-8b15-9cf422b60bba</Guid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8458	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8462	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8466	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 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 33 00 39 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>2022-05-23T05:29:39Z</CreationTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8564	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8568	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8570	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8610	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA3F4.tmp.WERInternalMetadata.xml	8614	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7DD.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1773b171\Report.wer	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1773b171\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	152	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_1773b171\Report.wer	9584	44	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 37 00 39 00 30 00 33 00 32 00 38 00 36 00 31 00 35 00	MetadataHash=790328615	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0df7dca4-87ea-295b-fb24-088f656e8197}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{0df7dca4-87ea-295b-fb24-088f656e8197}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{0df7dca4-87ea-295b-fb24-088f656e8197}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA607EE3FE	unknown

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

Analysis Process: WerFault.exe PID: **5436**, Parent PID: **3552**

General

Target ID:	13
Start time:	22:29:37
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3552 -s 332

Imagebase:	0x7ff76a840000
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	7FFA607F527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER235A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER235A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_15e02aea	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_15e02aea\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER235A.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER235A.tmp.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9052.tmp.csv	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER9082.tmp.txt	success or wait	1	7FFA607EE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 1b fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.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 50 25 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 7c fd fd 01 00 00 54 05 00 00 fd 03 00 00 fd 0d 00 00 fd 1b fd 62 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 02 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 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00	UBP%Lw|Tb0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	10276	1232	fd 43 19 06 fd 02 00 00 7d 45 40 71 fd 7f 00 00 00 00 73 fd fd 7f 00 00 fd 0b fd 07 fd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 06 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 2d fd fd 6e 00 00 00 00 73 fd fd 7f 00 00 00 00 73 fd fd 7f 00 00 00 00 73 fd fd 7f 00 00 28 fd 1f fd fd 00 00 00 fd fd 1f fd fd 00 00 00 fd 03 03 00 00 00 00 00 fd fd 1f fd fd 00 00 00 6e 5b 18 06 fd 02 00 00 0a 00 00 00 00 00 00 00 16 fd 66 4a fd 0f 00 00 fd fd fd fd fd fd fd 00 5b 18 06 fd 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 14 19 06 fd 02 00 00 fd 00 00 00 00 00 00	C}E@qs_3++S++-nsss(n[fJ[X	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	1632	168	0c 12 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	15204	20	52 00 00 00 00 42 18 06 fd 02 00 00 08 00 00 00 fd 40 00 00	RB@	success or wait	82	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	16520	8	fd fd 47 fd fd 00 00 00	G	success or wait	81	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	60740	8	fd 06 fd 73 fd 7f 00 00	s	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	11508	1232	28 fd 1f fd fd 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 38 fd 1f fd fd 00 00 00 fd fd fd fd fd fd fd 38 fd 1f fd fd 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 28 fd 1f fd fd 00 00 00 60 fd 1f fd fd 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 38 fd 1f fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 82 73 fd 7f 00	(3++S++F88(`8s	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	1900	48	1c 0f 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 20 33 fd fd 00 00 00 fd fd 4f fd fd 00 00 00 78 07 00 00 48 fd 00 00 fd 04 00 00 fd 36 00 00	3OxH6	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	9558	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	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	4556	4344	00 00 23 6e fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 0a 28 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 53 01 00 00 04 00 00 00 fd fd 73 fd 7f 00 00 fd fd 73 fd 7f 00 00 00 00 03 fd 01 00 00 00 fd fd fd 10 66 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 01 00 00 00 00 00	#n<2|h+(BB?#`A pSssfnS	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	8908	644	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 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 fd 02 00 00 00 00 00 50 fd 02 00 00 00 00 06 17 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 65 fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 fd 07 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 0a 06 00 00 00 00 00 1e fd fd 00 00 00 00 0c fd 1e 1e 00 00 00 00 4a fd 33 21 00 00 00 00 00 fd fd 0e 01 00 00 00 00 fd 28 01 00 fd 24 01 00 40 fd 05 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd 0a 06 00 fd fd 41 00 b2 01 00 4e 73 17 00 00 00 00 00 fd 5d 2c 00 5f 67 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 02 00	ZbPPe@J3!($@ANs],_g	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	60748	5464	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A8E.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 fd 10 00 00 38 12 00 00 05 00 00 00 24 05 00 00 64 3b 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	8$d;`8T"$	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 35 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3552</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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>00000000</CmdLineSignature>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 34 00 30 00 36 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>24068</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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 35 00 30 00 33 00 38 00 33 00 37 00 31 00 38 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 03837184 </PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.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 38 00 31 00 37 00 31 00 30 00 30 00 38 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>220340817 1008</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1626	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 33 00 31 00 31 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>26311</PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1712	100	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 31 00 30 00 35 00 30 00 31 00 37 00 33 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>105017344</PeakWorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1822	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 37 00 31 00 30 00 36 00 35 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>7106560</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	1912	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 36 00 39 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>106912</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2036	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 36 00 35 00 31 00 32 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>106512</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2144	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 32 00 32 00 38 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 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>22848</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2278	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 32 00 31 00 33 00 31 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21312</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2396	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 38 00 35 00 39 00 35 00 38 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>1859584</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2482	96	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 30 00 31 00 34 00 38 00 36 00 35 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101486592</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2588	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 38 00 35 00 39 00 35 00 38 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>1859584</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2668	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2720	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2768	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2806	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2810	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2814	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2870	4	0d 00 0a 00		success or wait	9	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2874	2	09 00		success or wait	18	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	2878	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 4a 00 74 00 4a 00 35 00 30 00 53 00 77 00 74 00 66 00 6f 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_JtJ50 Swtfo.dll</Parameter0>	success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	3670	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	3710	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	3714	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	3716	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	3754	4	0d 00 0a 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	3758	2	09 00		success or wait	12	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	3762	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4316	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4320	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4322	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4368	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4406	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4410	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4414	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4516	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 77 00 6b 00 63 00 73 00 71 00 6e 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>wkcsqn, Inc.</SystemManufacturer>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4630	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 77 00 6b 00 63 00 73 00 71 00 6e 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>wkcsqn7,1</SystemProductName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4726	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4730	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4734	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4862	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 30 00 37 00 32 00 34 00 30 00 34 00 39 00 37 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>1607240497</OSInstallDate>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4944	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4948	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	4952	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5054	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5058	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5062	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5130	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5134	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5136	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5176	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5180	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5182	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5216	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5220	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5224	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5320	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5324	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5326	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5362	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5366	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5368	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5392	4	0d 00 0a 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5396	2	09 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5400	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5652	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5656	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5658	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5684	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5688	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5690	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 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 34 00 36 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T05:29:46Z">	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5790	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5794	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	5798	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 34 00 31 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 35 00 35 00 32 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 33 00 37 00 36 00 35 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 33 00 37 00 36 00 35 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="414" PID="3552" UptimeMS="3765" TimeSinceCreationMS="3765" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6060	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6064	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6070	190	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 34 00 32 00 30 00 30 00 38 00 33 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 31 00 30 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="14200832" TimelineUnitShift="12" Timeline="110111"/>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6260	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6264	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6268	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6288	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6292	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6294	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6332	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6336	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6338	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6376	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6380	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6384	98	3c 00 47 00 75 00 69 00 64 00 3e 00 35 00 65 00 36 00 39 00 61 00 65 00 62 00 37 00 2d 00 30 00 64 00 62 00 61 00 2d 00 34 00 61 00 66 00 61 00 2d 00 39 00 36 00 65 00 63 00 2d 00 38 00 62 00 36 00 37 00 34 00 38 00 61 00 63 00 66 00 38 00 36 00 31 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>5e69aeb7-0dba-4afa-96ec-8b6748acf861</Guid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6482	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6486	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6490	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 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 34 00 36 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-23T05:29:46Z</CreationTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6588	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6592	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6594	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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6634	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2127.tmp.WERInternalMetadata.xml	6638	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	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER235A.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_15e02aea\Report.wer	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_15e02aea\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	152	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_JtJ_f1302aae73d1bd36c99beead2422e86237ae15_9903e0f3_15e02aea\Report.wer	9584	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 37 00 36 00 37 00 30 00 33 00 39 00 33 00 37 00 32 00	MetadataHash=-767039372	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0df7dca4-87ea-295b-fb24-088f656e8197}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{0df7dca4-87ea-295b-fb24-088f656e8197}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{0df7dca4-87ea-295b-fb24-088f656e8197}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA607EE3FE	unknown

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

Analysis Process: WerFault.exe PID: **5148**, Parent PID: **3552**

General

Target ID:	14
Start time:	22:29:38
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3552 -s 332

Imagebase:	0x7ff76a840000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5788**, Parent PID: **580**

General

Target ID:	16
Start time:	22:29:42
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **3008**, Parent PID: **580**

General

Target ID:	17
Start time:	22:29:52
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **4176**, Parent PID: **580**

General

Target ID:	22
Start time:	22:30:31
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: svchost.exe PID: **5328**, Parent PID: **580**

General

Target ID:	25
Start time:	22:31:18
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: svchost.exe PID: **6288**, Parent PID: **580**

General

Target ID:	26
Start time:	22:31:40
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

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: svchost.exe PID: **6908**, Parent PID: **580**

General

Target ID:	28
Start time:	22:31:59
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly