ID: 631906
Sample Name:
W3XqCWvDWC.dll
Cookbook: default.jbs
Time: 22:41:31
Date: 22/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

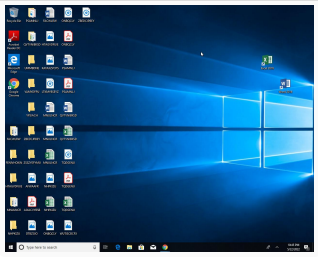
Windows Analysis Report

W3XqCWvDWC.dll

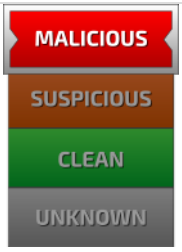
Overview

General Information

Sample Name:	W3XqCWvDWC.dll
Analysis ID:	631906
MD5:	661a35a77c5667..
SHA1:	81041189ebf61e..
SHA256:	1abc2d91d10d8a..
Tags:	exe trojan
Infos:	



Detection



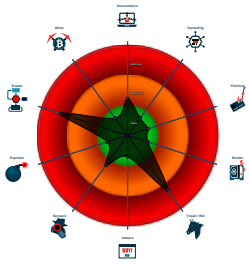
Emotet

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Multi AV Scanner detection for dom…
- 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 (…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7148 cmdline: loaddll64.exe "C:\Users\user\Desktop\W3XqCWvDWC.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6160 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\W3XqCWvDWC.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4668 cmdline: rundll32.exe "C:\Users\user\Desktop\W3XqCWvDWC.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 3608 cmdline: C:\Windows\system32\WerFault.exe -u -p 4668 -s 340 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - regsvr32.exe (PID: 6304 cmdline: regsvr32.exe /s C:\Users\user\Desktop\W3XqCWvDWC.dll MD5: D78B75FC68247E8A63ACBA846182740E)
      - regsvr32.exe (PID: 1012 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZDZEtulZzZAlvF\WFoCkDI.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
    - rundll32.exe (PID: 5156 cmdline: rundll32.exe C:\Users\user\Desktop\W3XqCWvDWC.dll,AddIn_FileTime MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 1836 cmdline: C:\Windows\system32\WerFault.exe -u -p 5156 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - rundll32.exe (PID: 4360 cmdline: rundll32.exe C:\Users\user\Desktop\W3XqCWvDWC.dll,AddIn_SystemTime MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 6520 cmdline: rundll32.exe C:\Users\user\Desktop\W3XqCWvDWC.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 6384 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6664 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6072 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6472 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5964 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4988 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6240 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.438067763.0000026206480000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.438652365.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.438097489.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.439554638.00000000003C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.451505642.0000018470750000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.3c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.18470750000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.18470750000.2.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.18470750000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.4f0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 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

Multi AV Scanner detection for domain / URL

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)

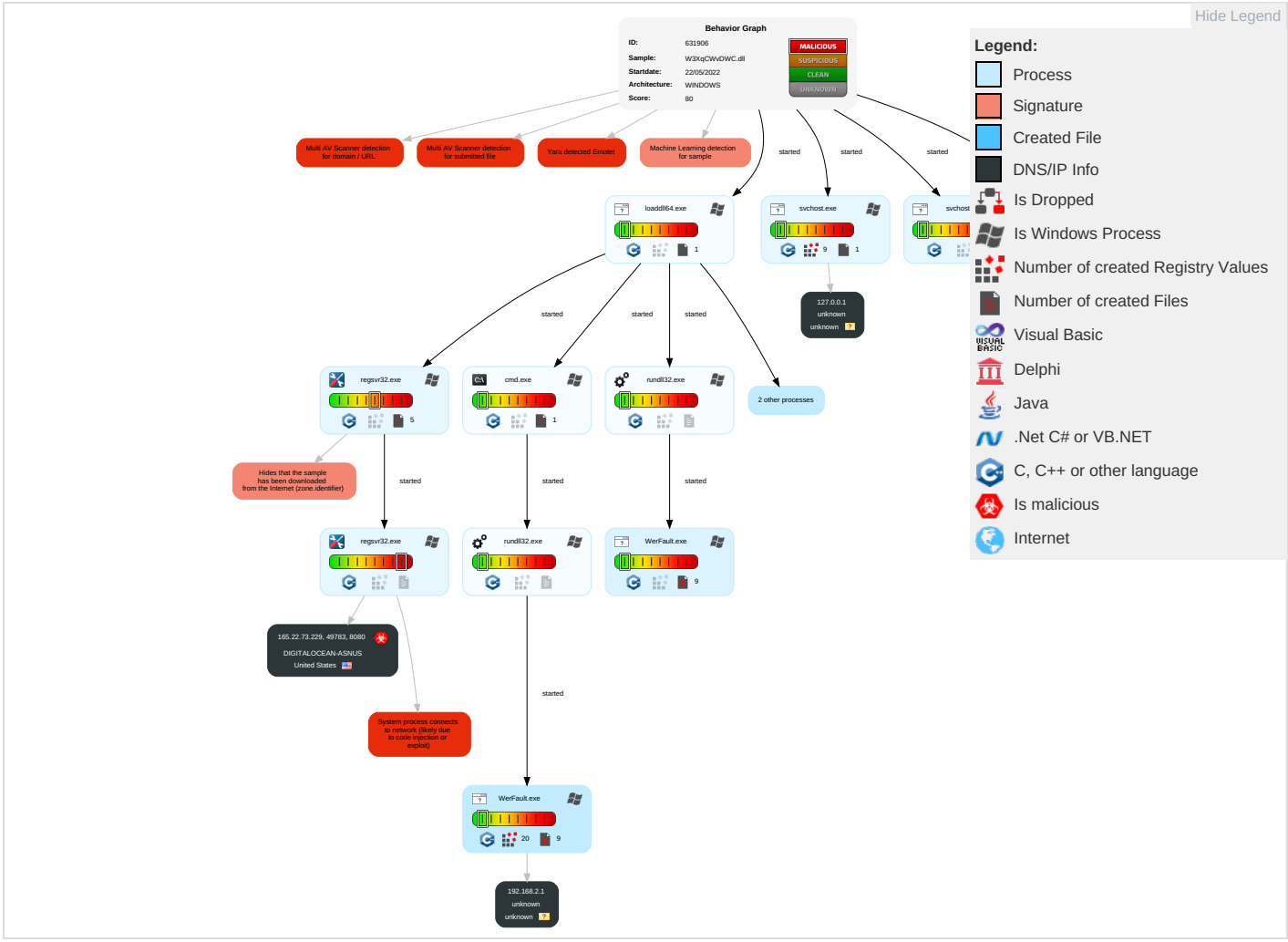
Stealing of Sensitive Information

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	3 Virtualization/Sandbox Evasion	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)	1 1 1 Process Injection	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 Deobfuscate/Decode Files or Information	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 Hidden Files and Directories	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	2 Obfuscated Files or Information	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	1 Regsvr32	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 Rundll32	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 DLL Side-Loading	/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 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

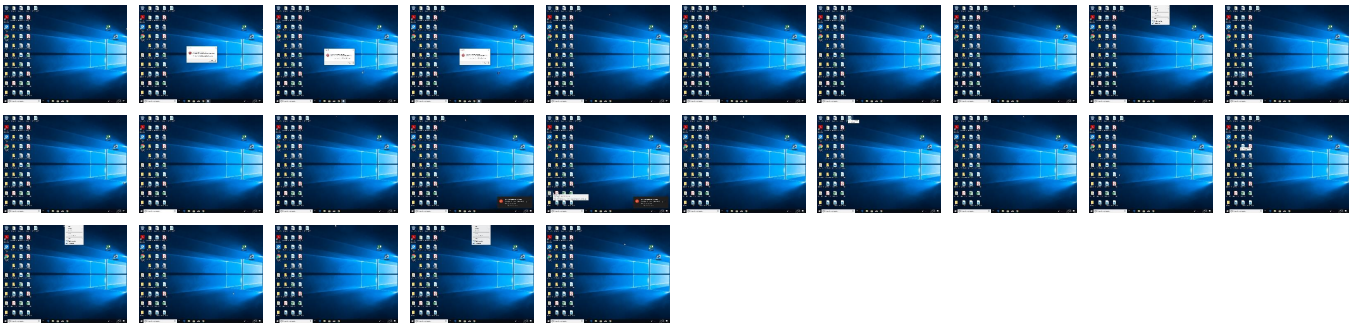
Behavior Graph



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
W3XqCWvDWC.dll	43%	Virustotal		Browse
W3XqCWvDWC.dll	59%	ReversingLabs	Win64.Trojan.Emotet	
W3XqCWvDWC.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.26206480000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.0.rundll32.exe.18470750000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.26206480000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.18470750000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
4.0.rundll32.exe.18470750000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.26206480000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.4f0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://165.22.73.229/BV	0%	Avira URL Cloud	safe	
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/	2%	Virustotal		Browse
http://https://165.22.73.229:8080/	0%	Avira URL Cloud	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://165.22.73.229/	7%	Virustotal		Browse
http://https://165.22.73.229/	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://165.22.73.229:8080/temsi	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://universalstore.streaming.mediaservices.windows	0%	Avira URL Cloud	safe	
http://https://165.22.73.229:8080/zU	0%	Avira URL Cloud	safe	
http://https://165.22.73.229:8080/t	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

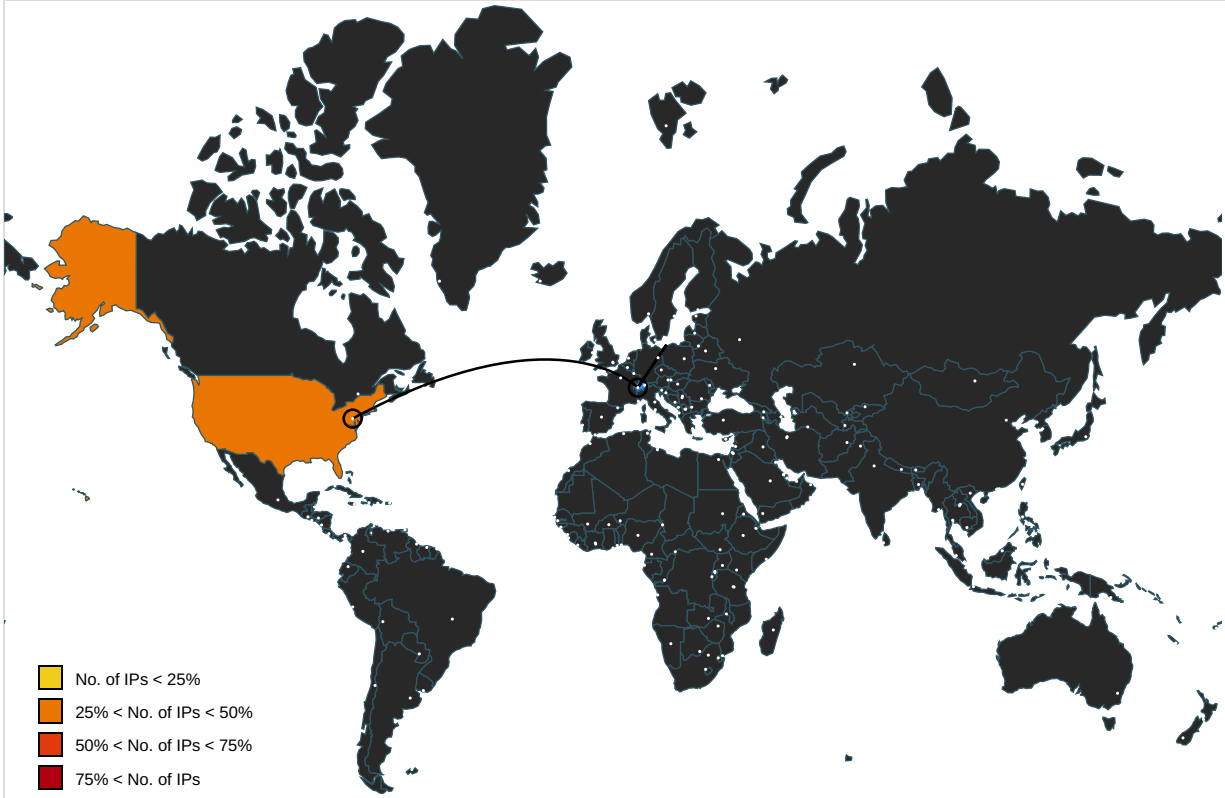
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://165.22.73.229/BV	regsvr32.exe, 00000008.00000003.50755828 0.00000000005D1000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 008.00000002.822895010.00000000005D1000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001B.00000003.671128536 .00000242A277D000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.671095428.00000242A279B000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001B.00000003.671128536 .00000242A277D000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.671095428.00000242A279B000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/	regsvr32.exe, 00000008.00000003.50755828 0.00000000005D1000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 008.00000002.822910866.00000000005E3000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.822895 010.00000000005D1000.00000004.00000020.0 0020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001B.00000003.666696840.00000242A27AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666628901.00000242A2C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666594098.00000242A279C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666649587.00000242A2C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666710075.00000242A2780000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666604195.00000242A27AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666734638.00000242A2C19000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000001B.00000003.666696840.00000242A27AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666628901.00000242A2C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666594098.00000242A279C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666649587.00000242A2C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666710075.00000242A2780000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666604195.00000242A27AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666734638.00000242A2C19000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001B.00000003.671128536.00000242A277D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.671095428.00000242A279B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229/	regsvr32.exe, 00000008.00000003.507558280.00000000005D1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.822895010.00000000005D1000.00000004.00000020.00020000.00000000.sdmp	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://crl.ver)	svchost.exe, 0000000F.00000002.777128497.0000024790464000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000002.694734206.00000242A1CE8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://165.22.73.229:8080/temsi	regsvr32.exe, 00000008.00000003.507558280.00000000005D1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.822910866.00000000005E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001B.00000003.674717470.00000242A2C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.674686049.00000242A27A3000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.674703615.00000242A277B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.674639892.00000242A27B9000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.674666781.00000242A27B9000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://universalstore.streaming.mediaservices.windows	svchost.exe, 0000001B.00000002.694834157.00000242A2728000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229:8080/zU	regsvr32.exe, 00000008.00000003.507558280.00000000005D1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.822895010.00000000005D1000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229:8080/t	regsvr32.exe, 00000008.00000003.507558280.00000000005D1000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.822910866.00000000005E3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://help.disneyplus.com.	svchost.exe, 0000001B.00000003.671128536.00000242A277D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.671095428.00000242A279B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.hotspotshield.com/	svchost.exe, 0000001B.00000003.666696840.00000242A27AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666628901.00000242A2C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666594098.00000242A279C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666649587.00000242A2C03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666710075.00000242A2780000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666604195.00000242A27AC000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.666734638.00000242A2C19000.00000004.00000020.00020000.00000000.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
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	631906

Start date and time: 22/05/202222:41:31	2022-05-22 22:41:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	W3XqCWvDWC.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	31
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:	mal80.troj.evad.winDLL@24/14@0/3
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:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.82.210.154, 20.189.173.22, 20.42.73.29, 20.40.136.238, 104.79.90.110, 40.112.88.60, 20.223.24.244
- Excluded domains from analysis (whitelisted): onedsblobprdwus17.westus.cloudapp.azure.com, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, onedsblobprdeus15.eastus.cloudapp.azure.com, sls.update.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, client.wns.windows.com, iris-de-prod-azsc-frc-b.francecentral.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, asf-ris-prod-neu.northeurope.cloudapp.azure.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.t
- 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.

Simulations

Behavior and APIs

Time	Type	Description
22:43:12	API Interceptor	1x 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):	0.2494083186559056
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4g:BJiRdwfu2SRU4g
MD5:	90571F728764E254F657D1CE42EBF9F4
SHA1:	198F2AF748E94FB0E4D6F578F21D48D8491E5261
SHA-256:	AD0810A6DAE43FACC006CCA7F16D42CAA1ED4F7C451A6283AD4F386656C62243
SHA-512:	91169248EC7AA08C6F5C412616CF4224EEB0865ED4CDC81FE3C5B6407CDB551A419504590E8976229841E9113DDFF27C5C7A5562723B028DD38373CE8E06576
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 0x30318109, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2506282112307677
Encrypted:	false
SSDEEP:	384:qff+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:qf0SB2nSB2RSjlK/+mLesOj1J2
MD5:	1B65E90BC63E649B4E738492CB80FD9C
SHA1:	8119E8D19440751583621D0AF6EB58DB37EF7036
SHA-256:	8B325A9B477E9B3565E9760F2F0A1D34C774F50544CF47154B5ACB1BE7DC03B1
SHA-512:	7ADE7F7646DB7724CB7D7091C9AC7E55C134C3AE747AEA59FB42C91677C63871FB1E952C5DEDFE99430C48F3A311C2FF6AA95A1AAA4D297D56AFE11819EAFB1C
Malicious:	false
Preview:	01..... .....e.f.3...w.....).....-...zw..+...z;.h.(.....-...zw...).....3...w.....B.....@..... ....-...zw.....i ..-...zw..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.0760895082623336
Encrypted:	false
SSDEEP:	3:AiR7voOgHQfU/l/NMqgYG64Kl//Z3Z/l/all3VkttlmlnI:hRroOgHQMHMqpG64u/ZpQ3
MD5:	FD31D092351B4356A1007DBA0D7036C6
SHA1:	1E793FBEC1AA51E2FB9307167675F10BC21D5538
SHA-256:	4DCC944301D7768459FC5B4791AF2B1BB96C55687B43F376844A2D59B0E59497
SHA-512:	AB4DF235C00E5A18683806BCB7EA07B7920462E83F725E6E3D438CA9CC974640337FCE2B3889072124F3D9E67F5EBD13DED17E4DD93BE1D1E2ED3F661DFC50B9
Malicious:	false
Preview:	*.T.....3...w...+...z;..-...zw.....-...zw..-...zw.8!Tv.-...z.o.....i ..-...zw..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_077be6ee\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):	0.7856130375317584
Encrypted:	false
SSDEEP:	96:vhFz7UiDJPnyjjv55od7Rl6tpXIQcQac6FcEocw3ZXaXz+HbHgSQgJPbOIDV9w8B:5poiDJKBHkBy9jg9/u7sWS274lt+I
MD5:	172D48FE973C999C3A84289ECCA83034
SHA1:	F8B511BAB5196B246F64482656984995A015047B
SHA-256:	3A627951D04A0E41B9051CC0B5A007AEF35E8DD650B95C2216097C12F58DA920
SHA-512:	76E2D920EFED11537E0DBB454ACE34716ED5FD7C0587BF0EF28A4060C8BE80072D55E03EF0BF95417582151C088C204A9281178B28A351D44CB7A63C89F78BEF
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.=.1.3.2.9.7.7.5.8.1.6.9.4.3.1.9.3.3.6.....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.=.1.3.2.9.7.7.5.8.1.7.1.7.2.8.8.0.1.4.....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.=.8.d.8.6.c.f.2.e.-.7.2.5.4.-.4.7.8.1.-.b.3.0.8.-.8.b.0.4.c.a.d.e.2.8.d.3... ..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.9.0.f.3.2.6.0.-.f.2.6.3.-.4.6.4.5.-.9.8.9.a.-.4.9.4.2.6.9.7.8.5.6.7.6.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.W.3.X.q.C.W.v.D.W.C...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.=.0.0.0.0.1.4.2.4.-.0.0.0.1.-.0.0.1.7.-.7.a.4.e.-.f.1.e.b.6.7.6.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_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_0e4fe7a9\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):	0.7847761768476103
Encrypted:	false
SSDEEP:	96:IpiFreUiKJPnyqjv55od7Rl6tpXIQcQac6FcEocw3ZXaXz+HbHgSQgJPbOIDV9wA:XxhiKJKQHkBy9jg9/u7sWS274lt+l
MD5:	1546D7CFC882245A30F9986FBCD21675
SHA1:	98B12BB2164B156E3C69630E623AC47FE69491DE
SHA-256:	55BE21B2D63B74884B1B32AB2E282AC05E95C0DFFB305A59A5A0E5DBA1783398
SHA-512:	9807B7AFB63F8021661C56F2681D45547CC8FE50B79755110FC451634F4C98EF2BBABB7465B1548279F7E159D0813B8D36C3C82A97AD410B218AFCCB112A92AD
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.=.1.3.2.9.7.7.5.8.1.6.9.2.6.8.8.3.1.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.5.8.1.7.1.5.8.1.3.1.5.6.....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.c.1.3.d.b.f.3.-.6.a.5.4.-.4.7.c.4.-.b.f.d.b.-.9.f.2.3.e.8.9.c.e.1.f.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.=.9.f.3.a.1.7.7.a.-.0.1.a.6.-.4.e.7.6.-.a.0.6.8.-.5.f.7.9.7.9.a.c.3.b.e.a.....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._.W.3.X.q.C.W.v.D.W.C...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.=.0.0.0.0.1.2.3.c.-.0.0.0.1.-.0.0.1.7.-.f.9.4.9.-.b.a.e.b.6.7.6.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\WERD838.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 05:42:49 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64540
Entropy (8bit):	2.3110621449378694
Encrypted:	false
SSDEEP:	384:Z04cSe2YqH2DSC2Fffv54cldYnZrEQz214mRb:ZfMqH2DSCuffv54+7QI
MD5:	2B3D870F5E039ED2FD094BF6AB0F888E
SHA1:	67F812631E393D2CCA53DCF67C150B349052E2A4
SHA-256:	10DA7FF50539CC55A83B09BEC8EAC853D0AB65AD9435FFB912FC77A1B328F3B5
SHA-512:	1B518B5EABFD9FA3685C4417ADC0DC04BFF6F8E22AC998C8263EDA76F2AA8AE86A55EB2C704079003DF03B7777FC077F1EDFDE0BBF0C54DE7F91A5A7160FA587
Malicious:	false
Preview:	MDMP..... .....b.....8.....$...d;.....`.....8.....T.....t.....".....$.....U.....B.....P%... ...Lw.....Z.....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\WERD8D4.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 05:42:50 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64680
Entropy (8bit):	2.3029438228682264
Encrypted:	false
SSDEEP:	192:hVJF04cqPyowuCSrMV/qkm+s494+nzOC5IOTiaOaHXdOYXqf1XItVmiqwkseJeNs:D04cSe2YqH2qC2sjcldYnqyUGvU
MD5:	BA90AEF54026CA309698E50A4696514C
SHA1:	3B8E22FDEB17257CDDA5545B0BC3297156C2A54C
SHA-256:	83B71B4EFDAA26420AD43DA28FD9BBD25659BE604A0D2F33383C5878BA2A5BFD
SHA-512:	1225DF3D6A15E29AB8056D12F65535AA32474B0E4F58946AFDFA26F614444BE296A0E78BD9A0EC190EF2F4A29B4D0CCC53C8B88F27E69109261DF62B8948D1DE
Malicious:	false
Preview:	MDMP..... .....b.....8.....4...d;.....`.....8.....T.....X...P.....".....$.....U.....B.....P%... ...Lw.....A.....T.....$.....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\WERDCBD.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):	8646
Entropy (8bit):	3.698531447554491

Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiRxcUBaKV6Y6QDEFgmf82SeCpr389bC/0fx2m:RrlsNi3cUBaKV6YVDEFgmf82SOCMfJ
MD5:	FABF2607A8361E53D7CBB554668A653D
SHA1:	01FB6AD0C2F1FE435C5AB498C4FEAD7A144C6C63
SHA-256:	58A9D32FA2C8F9FE51C9B7D8AA994A2535B35CAF7A933E6C955A810F5FEA7645
SHA-512:	FB7A9BD3317B0C6C50B062C158D6A50DFB8944D296638FF64F3AA988B7A850A1A1720790F52383584B6D10739FD08E4070147781B1311F609BB025B571C7825D
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.>.4.6.6.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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):	8642
Entropy (8bit):	3.6980480457086395
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiicgUlaDk6YDbbgmf82SeCprA89bC1hfgL2m:RrlsNiBgUlaDk6Yfbgmf82S7CDfq
MD5:	DE3315F831F537C0FE2289B4B9C43CD2
SHA1:	131B5D032F0313CE6CDE04960305C3F0D90702A5
SHA-256:	15ED2F6EF5E92090EBA6A87EC99B518BBD328BC9DC4DD7DDE0BCCBE5BD6EE5F0
SHA-512:	B08FFA32B791AD3C7B592872A0A7B9960547FEDD0FF04103E1A4CFBC53CD09CF1C3F48D4AB3041738F8B4DE427E886B26212C2C86974B197F22E87B800739BF
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.>.5.1.5.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDEE1.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):	4.507451445102132
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtBI9DzWgc8sqYjrB8fm8M4JCqC9fknFz9yq8vh9fk0XZESC5S6d:uITflJCgrsqYvGJt9WHVv6d
MD5:	D3EE6D18BABB00892BEC4095648E8D29
SHA1:	407BA521751D26FC32281466C2764BC0FDCF5D89
SHA-256:	E322EAC18B80DE52D8CD519814EA6F55370CF5951654BE0115CFB23D69DBA99B
SHA-512:	A569574ECAD0525333A7FF204D5A71185A8202FC47ACCA011589C6423D5AB4AF0819EAABA01306522639F137C0CC73BDCC280B1CCFAB46DACC3BA5B74C72BC0
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="1527293" />.. <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\WERE01A.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):	4.50987212751965
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLJgtBI9DzWgc8sqYjx8fm8M4JCqC9fknF4MWyRyq8vh9fk1ZESC5SNd:uITflJCgrsqYyJUyRWuVvNd
MD5:	7B08DBE174F6DAD749693867D428410F

SHA1:	37FAA847734D00220A74C2F68B97F6F2D22A50D6
SHA-256:	8D4D648575C3D2FC98C8BE927543F53DEF89433FC042C33D23F3911B3224F83F
SHA-512:	76112FA097D114B5FE44447A1B696496B0A0FE1EDACC593FBCF8D48ED06DCAEF32CF8167BFB62CAC3C465D2B1624EAFC2B0438B1A8FAC25CC0C4F15475E52294
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="1527293" />.. <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\Logs\waasmedic\waasmedic.20220308_162907_174.etl

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	1.544091868845645
Encrypted:	false
SSDEEP:	48:85Or524NFrkyNb7kUMb7kENmb7kl9b7k9W:724NFrka0UM0f0L09W
MD5:	5254329BC871F6ABF4A79949F6DE1ABD
SHA1:	FFA9498CF8C1D2AF1695CB3756ECE482309C0C40
SHA-256:	BC45C493581B97B2130962F1D9BE1221A5D39FF44560BA40278E7D91E13C8A21
SHA-512:	73A8DE6B61E02BC7E12C3294876F040CD8306FBC87795B0A7DF863CB2E11CE51C284033A0465AB8A9AAF85AB9C4B8EE178EB12830654CC1D69D1F374A4E6729
Malicious:	false
Preview:	.....!.....`....'.....B.....Rhn..Zb..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.2.....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....5.3.... .....L.hn.....E.C.C.B.1.7.5.F.-.1.E.B.2.-.4.3.D.A.-.B.F.B.5.-.A.8.D.5.8.A.4.0.A.4.D.7...C.:.\.W.i.n.d.o.w.s.\.l.o.g.s.\.w.a.a.s.m.e.d.i.c.\.w.a.a.s.m.e.d.i.c...2.0.2.2.0.3.0.8._.1.6.2.9.0.7._.1.7.4...e.t.l.....P.P.....`....'.....9.B...'....17134.1.amd64fre.rs4_release.180410-1804.....5.@...'....OYo."(.s..O.....WaaSMedicSvc.pdb.....

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):	7.152712651608759
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:	W3XqCWvDWC.dll
File size:	371200
MD5:	661a35a77c56679722f7180fc4add7ba
SHA1:	81041189ebf61ed4220f4cea933465cc28d48f57

SHA256:	1abc2d91d10d8a44bcc6ce69334f992e5304f3dcb48fe8328d888a25f3228c8d
SHA512:	94a66112e36647502419843e4f577b454c4f341616a580f029cb5c3e8decd9b07077ed16e158b0c029eaf04bb7fcbb7218120af76033749ba93203548235646f
SSDEEP:	6144:hlNuuXQASByX7/xoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7Fy/BJ7rGTK/V3
TLSH:	C1848E46F7F551E5E8F7C13889A23267F9317C948B38A7CB8A44466A4F70BA0E93D701
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 00007FE0D8C0F997h
call 00007FE0D8C14CF7h
dec esp
mov eax, dword ptr [esp+40h]
mov edx, dword ptr [esp+38h]
dec eax
mov ecx, dword ptr [esp+30h]
call 00007FE0D8C0F9A4h
dec eax
add esp, 28h
ret
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
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 00007FE0D8C0F9A2h
cmp dword ptr [00028DE8h], 00000000h
jne 00007FE0D8C0F999h
xor eax, eax
jmp 00007FE0D8C0FAB4h
cmp dword ptr [esp+58h], 01h
je 00007FE0D8C0F999h
cmp dword ptr [esp+58h], 02h
jne 00007FE0D8C0F9E0h
dec eax
cmp dword ptr [0001ED99h], 00000000h
je 00007FE0D8C0F9AAh
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 00007FE0D8C0F9A9h
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call 00007FE0D8C0F6FAh
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
jne 00007FE0D8C0F999h
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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x2f000	0xfcc	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5f000	0x294	.reloc
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	0.275474330357	data	4.41581052225	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**
English	United States	

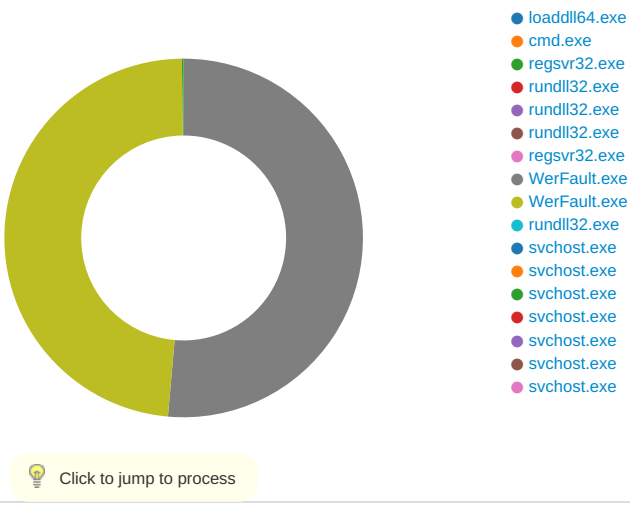
Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 22:43:19.709748030 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:19.753823042 CEST	8080	49783	165.22.73.229	192.168.2.5
May 22, 2022 22:43:19.753973007 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:19.793998957 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:19.838298082 CEST	8080	49783	165.22.73.229	192.168.2.5
May 22, 2022 22:43:19.850178957 CEST	8080	49783	165.22.73.229	192.168.2.5
May 22, 2022 22:43:19.850240946 CEST	8080	49783	165.22.73.229	192.168.2.5
May 22, 2022 22:43:19.850332975 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:19.850414038 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:20.462939978 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:20.506202936 CEST	8080	49783	165.22.73.229	192.168.2.5
May 22, 2022 22:43:20.506323099 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:20.510158062 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:20.596313000 CEST	8080	49783	165.22.73.229	192.168.2.5
May 22, 2022 22:43:20.762878895 CEST	8080	49783	165.22.73.229	192.168.2.5
May 22, 2022 22:43:20.764266014 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:23.763127089 CEST	8080	49783	165.22.73.229	192.168.2.5
May 22, 2022 22:43:23.763151884 CEST	8080	49783	165.22.73.229	192.168.2.5
May 22, 2022 22:43:23.763258934 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:43:23.763273954 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:45:09.634879112 CEST	49783	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:45:09.634922981 CEST	49783	8080	192.168.2.5	165.22.73.229

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 7148, Parent PID: 4908

General

Target ID:	0
Start time:	22:42:41
Start date:	22/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\W3XqCWvDWC.dll"
Imagebase:	0x7ff79aa30000
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: 6160, Parent PID: 7148

General

Target ID:	1
Start time:	22:42:41
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\W3XqCWvDWC.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: 6304, Parent PID: 7148

General

Target ID:	2
Start time:	22:42:42
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\W3XqCWvDWC.dll

Imagebase:	0x7ff731d30000
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: 00000002.00000002.439554638.00000000003C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.440213719.0000000180001000.00000020.00001000.00020000.00000000.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\ZDZEtulZzZAlvF\WFoCkDI.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: **4668**, Parent PID: **6160**

General

Target ID:	3
Start time:	22:42:42
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\W3XqCWvDWC.dll",#1
Imagebase:	0x7ff760ae0000
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: 00000003.00000000.438067763.0000026206480000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.439023935.0000026206480000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.438864960.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.451930220.0000026206480000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.437812293.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.451719262.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **5156**, Parent PID: **7148**

General

Target ID:	4
Start time:	22:42:42
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\W3XqCWvDWC.dll,AddIn_FileTime

Imagebase:	0x7ff760ae0000
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: 00000004.00000000.438652365.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.438097489.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.451505642.0000018470750000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.438883256.0000018470750000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.438175945.0000018470750000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.451269491.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **4360**, Parent PID: **7148**

General

Target ID:	5
Start time:	22:42:46
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\W3XqCWvDWC.dll,AddIn_SystemTime
Imagebase:	0x7ff760ae0000
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: regsvr32.exe PID: **1012**, Parent PID: **6304**

General

Target ID:	8
Start time:	22:42:46
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZDZEtuIZzZAlvF\WFoCkDI.dll"
Imagebase:	0x7ff731d30000
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: 00000008.00000002.822761253.00000000004F0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.823478736.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

Reputation:	high

Analysis Process: WerFault.exe PID: **3608**, Parent PID: **4668**

General

Target ID:	9
Start time:	22:42:48
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 4668 -s 340
Imagebase:	0x7ff76a840000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA607F527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.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\WERD838.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\WERDCBD.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\WERDCBD.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\WERDEE1.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\WERDEE1.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_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_0e4fe7a9	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_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_0e4fe7a9\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\WERD838.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDEE1.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	success or wait	1	7FFA607EE9F7	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDEE1.tmp.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D51.tmp.csv	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D71.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\WERD838.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 1e fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.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 5a fd fd 01 00 00 54 05 00 00 fd 03 00 00 3c 12 00 00 fd 1e 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%LwZT<b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	10276	1232	fd fd 3f fd 00 00 40 14 23 6e fd 7f 00 00 00 00 fd 60 fd 7f 00 00 7d 45 40 71 fd 7f 00 00 fd 01 0a 00 00 00 00 00 fd 0b 51 06 62 02 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 39 04 46 fd 6e 00 00 00 00 fd 60 fd 7f 00 00 00 00 fd 60 fd 7f 00 00 00 00 fd 60 fd 7f 00 00 fd fd fd 74 fd 00 00 00 20 fd fd 74 fd 00 00 00 fd 01 0a 00 00 00 00 00 78 fd fd 74 fd 00 00 00 16 53 29 06 62 02 00 00 0a 00 00 00 00 00 00 00 28 62 fd 4c fd 0f 00 00 fd fd fd fd fd fd fd fd 52 29 06 62 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 11 2a 06 62 02 00 00 fd 00 00 00 00 00 00	? @#n`}E@qQb_3++S++9 Fn```t txtS)b(bLR)bX*b	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	1632	168	40 18 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 fd 04 00 00 24 28 00 00	@$(	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	15204	20	52 00 00 00 18 fd 2f 75 fd 00 00 00 fd 09 00 00 fd 40 00 00	R/u@	success or wait	82	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	16520	2536	76 fd 7a 73 fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 7b 73 fd 7f 00 00 10 00 00 00 00 00 00 00 58 fd 2f 75 fd 00 00 00 51 fd 2f 75 fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 50 0c 75 fd 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 10 46 2a 06 62 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 48 30 29 06 62 02 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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`2{sX/uQ/uPuF*bH0)bXX	success or wait	81	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	59188	8	50 fd 2f 75 fd 00 00 00	P/u	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	11508	1232	fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd 74 fd 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 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 fd fd fd 74 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd 74 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 28 fd fd 74 fd 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 74 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	t 3++S++Ftt(tts	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	1900	48	00 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 0c 75 fd 00 00 00 18 fd 2f 75 fd 00 00 00 fd 09 00 00 fd 40 00 00 fd 04 00 00 fd 36 00 00	u/u@6	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.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\WERD838.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 11 22 fd fd 67 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 pSss"gnS	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.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 40 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 44 0b 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 1c fd 03 00 00 00 00 00 00 00 00 00 00 00 00 fd 14 1b 00 00 00 00 00 74 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 44 06 06 00 00 00 00 00 fd fd 1f 00 00 00 00 48 fd 48 1d 00 00 00 00 fd 79 fd 20 00 00 00 00 fd 74 6c 01 00 00 00 00 0b 23 01 00 50 0d 01 00 fd fd 05 00 fd fd 0a 00 74 fd 04 00 06 7f 15 00 44 06 06 00 7b 45 2f 00 fd fd 01 00 00 fd 13 00 00 00 00 00 0b fd 1c 00 07 67 04 00 43 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 02 00	Zb@Dt@DHHy tl#PtD{E/gC	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD838.tmp.dmp	59196	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\WERD838.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 74 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$d;`8Tt"$	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 36 00 36 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4668</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.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\WERDCBD.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 31 00 32 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8128</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1228	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\WERDCBD.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1314	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\WERDCBD.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1374	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\WERDCBD.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1428	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 37 00 39 00 32 00 31 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>2203503792128</PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1534	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\WERDCBD.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1624	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 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>26292</PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1710	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\WERDCBD.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1820	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\WERDCBD.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	1910	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 35 00 35 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>106552</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2028	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\WERDCBD.tmp.WERInternalMetadata.xml	2034	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 33 00 35 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>106352</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2136	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2142	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 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21536</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2266	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2270	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2276	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 31 00 38 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>21184</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2384	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2388	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2394	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 32 00 36 00 38 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1826816</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2474	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\WERDCBD.tmp.WERInternalMetadata.xml	2480	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 32 00 30 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101462016</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2586	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 32 00 36 00 38 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1826816</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2666	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\WERDCBD.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2720	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\WERDCBD.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2760	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\WERDCBD.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 36 00 31 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6160</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2846	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\WERDCBD.tmp.WERInternalMetadata.xml	2854	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\WERDCBD.tmp.WERInternalMetadata.xml	2914	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2918	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	2926	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\WERDCBD.tmp.WERInternalMetadata.xml	3016	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3020	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3028	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 36 00 34 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8640</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3070	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3074	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3082	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\WERDCBD.tmp.WERInternalMetadata.xml	3160	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3164	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3172	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\WERDCBD.tmp.WERInternalMetadata.xml	3224	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3228	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3236	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\WERDCBD.tmp.WERInternalMetadata.xml	3280	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3284	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3294	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 33 00 36 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203370369024</PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3404	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 33 00 36 00 39 00 30 00 32 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203370369024</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3498	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 38 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>789</PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3584	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 33 00 36 00 38 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2936832</PeakWorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3684	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\WERDCBD.tmp.WERInternalMetadata.xml	3694	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 39 00 33 00 36 00 38 00 33 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>29368 32</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3774	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3788	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	<QuotaPeakPagedPoolU sage>27840 </QuotaPeakPagedPool Usage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3900	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3904	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	3914	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 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 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</Qu otaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4024	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	<QuotaPeakNonPagedP oolUsage>42 08</QuotaPeakNonPage dPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4146	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4150	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\WERDCBD.tmp.WERInternalMetadata.xml	4160	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 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>3800</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4280	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 33 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3133440</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4370	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\WERDCBD.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4476	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 33 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3133440</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4560	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\WERDCBD.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4610	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\WERDCBD.tmp.WERInternalMetadata.xml	4616	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\WERDCBD.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4666	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\WERDCBD.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4704	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\WERDCBD.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4752	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\WERDCBD.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4798	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\WERDCBD.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	4862	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 57 00 33 00 58 00 71 00 43 00 57 00 76 00 44 00 57 00 43 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_W3XqCWvDWC.dll</Parameter0>	success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	5648	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	5652	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\WERDCBD.tmp.WERInternalMetadata.xml	5654	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\WERDCBD.tmp.WERInternalMetadata.xml	5694	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	5698	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	5700	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\WERDCBD.tmp.WERInternalMetadata.xml	5738	4	0d 00 0a 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	5742	2	09 00		success or wait	12	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	5746	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\WERDCBD.tmp.WERInternalMetadata.xml	6300	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6304	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6306	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\WERDCBD.tmp.WERInternalMetadata.xml	6346	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6350	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6352	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\WERDCBD.tmp.WERInternalMetadata.xml	6390	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6394	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6398	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\WERDCBD.tmp.WERInternalMetadata.xml	6492	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6496	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\WERDCBD.tmp.WERInternalMetadata.xml	6500	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 6a 00 77 00 6c 00 72 00 68 00 65 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>jwlrhe, Inc.</SystemManufacturer>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6606	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6610	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6614	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 6a 00 77 00 6c 00 72 00 68 00 65 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>jwlrhe7,1</SystemProductName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6710	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6714	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6718	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\WERDCBD.tmp.WERInternalMetadata.xml	6838	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6842	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6846	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 31 00 38 00 39 00 37 00 32 00 36 00 31 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1618972613</OSInstallDate>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6928	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	6932	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\WERDCBD.tmp.WERInternalMetadata.xml	6936	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\WERDCBD.tmp.WERInternalMetadata.xml	7038	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7042	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7046	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\WERDCBD.tmp.WERInternalMetadata.xml	7114	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7118	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7120	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\WERDCBD.tmp.WERInternalMetadata.xml	7160	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7164	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7166	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\WERDCBD.tmp.WERInternalMetadata.xml	7200	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7204	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7208	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7304	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7308	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7310	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\WERDCBD.tmp.WERInternalMetadata.xml	7346	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7350	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7352	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\WERDCBD.tmp.WERInternalMetadata.xml	7376	4	0d 00 0a 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7380	2	09 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7384	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\WERDCBD.tmp.WERInternalMetadata.xml	7630	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7634	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7636	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\WERDCBD.tmp.WERInternalMetadata.xml	7662	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7666	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7668	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 34 00 32 00 3a 00 35 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T05:42:50Z">	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7768	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	7772	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\WERDCBD.tmp.WERInternalMetadata.xml	7776	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 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 36 00 36 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 37 00 33 00 34 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 33 00 34 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="416" PID="4668" UptimeMS="3734" TimeSinceCreationMS="3734" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8038	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8042	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8048	180	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 35 00 35 00 35 00 34 00 31 00 37 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5554176" TimelineUnitShift="12" Timeline="11"/>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8228	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8232	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8236	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\WERDCBD.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8260	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8262	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\WERDCBD.tmp.WERInternalMetadata.xml	8300	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8304	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8306	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\WERDCBD.tmp.WERInternalMetadata.xml	8344	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8348	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8352	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 63 00 31 00 33 00 64 00 62 00 66 00 33 00 2d 00 36 00 61 00 35 00 34 00 2d 00 34 00 37 00 63 00 34 00 2d 00 62 00 66 00 64 00 62 00 2d 00 39 00 66 00 32 00 33 00 65 00 38 00 39 00 63 00 65 00 31 00 66 00 30 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>3c13dbf3-6a54-47c4-bfdb-9f23e89ce1f0</Guid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8450	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8454	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8458	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 34 00 32 00 3a 00 35 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-23T05:42:50Z</CreationTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8556	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8560	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8562	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\WERDCBD.tmp.WERInternalMetadata.xml	8602	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDCBD.tmp.WERInternalMetadata.xml	8606	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\WERDEE1.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 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_0e4fe7a9\Report.wer	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_0e4fe7a9\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_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_0e4fe7a9\Report.wer	9584	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 34 00 32 00 33 00 37 00 38 00 36 00 34 00 36 00 33 00	MetadataHash=-1423786463	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: WerFault.exe PID: **1836**, Parent PID: **5156**

General

Target ID:	10
Start time:	22:42:48
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 5156 -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
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA607F527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.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\WERD8D4.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\WERDD88.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\WERDD88.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\WERE01A.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\WERE01A.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_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_077be6ee	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_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_077be6ee\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\WERD8D4.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE01A.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE01A.tmp.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E1E.tmp.csv	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E3E.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\WERD8D4.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 1e fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.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\WERD8D4.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 41 01 fd 01 00 00 54 05 00 00 fd 03 00 00 24 14 00 00 fd 1e 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%LwAT$b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	10276	1232	00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 fd 60 fd 7f 00 00 40 14 23 6e fd 7f 00 00 fd 37 65 70 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 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 fd fd 38 3e 71 6e 00 00 00 00 fd 60 fd 7f 00 00 00 00 fd 60 fd 7f 00 00 00 00 fd 60 fd 7f 00 00 fd fd fd 0c 14 00 00 00 30 fd fd 0c 14 00 00 00 16 02 0c 00 00 00 00 00 fd fd fd 0c 14 00 00 00 6a 5b 64 70 fd 01 00 00 0a 00 00 00 00 00 00 00 28 62 fd 4c fd 0f 00 00 fd fd fd fd fd fd fd 00 5b 64 70 fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 10 65 70 fd 01 00 00 fd 00 00 00 00 00 00	`@#n7ep}E@q_3++S++8>qn```0j[dp(bL[dpep	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	1632	168	fd 11 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 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	15204	20	53 00 00 00 00 fd 02 fd 01 00 00 00 06 00 00 00 fd 40 00 00	S@	success or wait	83	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	16536	6	01 04 01 00 04 22	"	success or wait	82	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	49644	9800	fd 57 fd 6f fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 fd 0c 14 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Wo H	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	11508	1232	fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd 0c 14 00 00 00 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 fd fd 0c 14 00 00 00 fd fd fd fd fd fd fd fd fd fd 0c 14 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 fd 0c 14 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 0c 14 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++F(s	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	1900	48	fd 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 fd 0c 14 00 00 00 58 fd fd 0c 14 00 00 00 fd 04 00 00 3c fd 00 00 fd 04 00 00 fd 36 00 00	pX<6	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.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\WERD8D4.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 21 12 fd 67 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 pSss!gnS	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.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 50 fd 02 00 00 00 00 00 fd fd 02 00 00 00 00 56 0b 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 fd 03 00 00 00 00 00 1c fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 1c 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 44 06 06 00 00 00 00 00 fd fd 1f 00 00 00 00 fd 11 4b 1d 00 00 00 00 77 fd fd 20 00 00 00 00 fd fd 6c 01 00 00 00 00 3d 23 01 00 4f 0e 01 00 fd fd 05 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 44 06 06 00 4b 7e 2f 00 fd fd 01 00 0b fd 13 00 00 00 00 00 5a fd 1c 00 1e 67 04 00 49 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 02 00	ZbPV[@DKw l=#ODK~/ZgI	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD8D4.tmp.dmp	59444	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\WERD8D4.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 34 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 50 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	84d;`8TXP"$	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 31 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5156</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.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\WERDD88.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 39 00 37 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7977</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1228	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\WERDD88.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1310	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\WERDD88.tmp.WERInternalMetadata.xml	1314	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\WERDD88.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1374	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\WERDD88.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1428	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 38 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 03808512 </PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1534	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\WERDD88.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1624	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 38 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>26286 </PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1704	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\WERDD88.tmp.WERInternalMetadata.xml	1710	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\WERDD88.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1820	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\WERDD88.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	1910	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 35 00 35 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>106552</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2028	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2034	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 33 00 35 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>106352</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2136	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\WERDD88.tmp.WERInternalMetadata.xml	2142	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 34 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 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>21440</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2266	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2270	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2276	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 30 00 38 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>21088</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2384	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2388	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2394	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 31 00 38 00 36 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1818624</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2474	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2480	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 35 00 33 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101453824</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2580	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\WERDD88.tmp.WERInternalMetadata.xml	2586	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 31 00 38 00 36 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1818624</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2666	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\WERDD88.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2720	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\WERDD88.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2760	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\WERDD88.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7148</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2846	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2854	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 36 00 34 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll64.exe</ImageName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2926	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	2930	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\WERDD88.tmp.WERInternalMetadata.xml	2938	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3028	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3032	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3040	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 34 00 32 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9426</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3082	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3086	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3094	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\WERDD88.tmp.WERInternalMetadata.xml	3172	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3176	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3184	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\WERDD88.tmp.WERInternalMetadata.xml	3236	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3240	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3248	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\WERDD88.tmp.WERInternalMetadata.xml	3292	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3296	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\WERDD88.tmp.WERInternalMetadata.xml	3306	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 34 00 35 00 31 00 31 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4345114624</PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3396	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3400	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3410	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 34 00 31 00 31 00 34 00 39 00 36 00 39 00 36 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>4341149696</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3498	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 33 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>639</PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3584	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 33 00 31 00 34 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2314240</PeakWorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3694	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 33 00 30 00 36 00 30 00 34 00 38 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>2306048</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3774	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\WERDD88.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3788	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 38 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 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>28208</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3900	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3904	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	3914	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>20448</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4024	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>4072</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4146	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4150	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4160	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 38 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>2984</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4266	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\WERDD88.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4280	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 36 00 39 00 34 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>466944</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4368	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 31 00 30 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>471040</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4458	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4462	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4472	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 36 00 36 00 39 00 34 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>466944</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4542	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4546	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4554	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\WERDD88.tmp.WERInternalMetadata.xml	4600	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4604	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4610	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\WERDD88.tmp.WERInternalMetadata.xml	4652	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4656	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4660	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4692	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4696	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4698	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\WERDD88.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4746	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\WERDD88.tmp.WERInternalMetadata.xml	4784	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4788	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4792	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\WERDD88.tmp.WERInternalMetadata.xml	4848	4	0d 00 0a 00		success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4852	2	09 00		success or wait	18	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	4856	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 57 00 33 00 58 00 71 00 43 00 57 00 76 00 44 00 57 00 43 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_W3XqCWvDWC.dll</Parameter0>	success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	5642	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	5646	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	5648	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\WERDD88.tmp.WERInternalMetadata.xml	5688	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	5692	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	5694	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	5732	4	0d 00 0a 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	5736	2	09 00		success or wait	12	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	5740	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\WERDD88.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6300	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\WERDD88.tmp.WERInternalMetadata.xml	6340	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6344	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6346	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\WERDD88.tmp.WERInternalMetadata.xml	6384	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6388	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6392	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\WERDD88.tmp.WERInternalMetadata.xml	6486	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6490	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6494	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 6a 00 77 00 6c 00 72 00 68 00 65 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>jwlrhe, Inc.</SystemManufacturer>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6600	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\WERDD88.tmp.WERInternalMetadata.xml	6604	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6608	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 6a 00 77 00 6c 00 72 00 68 00 65 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>jwlrhe7,1</SystemProductName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6704	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6708	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6712	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\WERDD88.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6840	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 31 00 38 00 39 00 37 00 32 00 36 00 31 00 33 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1618972613</OSInstallDate>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6922	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6926	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	6930	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\WERDD88.tmp.WERInternalMetadata.xml	7032	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7036	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\WERDD88.tmp.WERInternalMetadata.xml	7040	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\WERDD88.tmp.WERInternalMetadata.xml	7108	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7112	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7114	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\WERDD88.tmp.WERInternalMetadata.xml	7154	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7158	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7160	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\WERDD88.tmp.WERInternalMetadata.xml	7194	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7198	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7202	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7298	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7302	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7304	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\WERDD88.tmp.WERInternalMetadata.xml	7340	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7344	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7346	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\WERDD88.tmp.WERInternalMetadata.xml	7370	4	0d 00 0a 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7374	2	09 00		success or wait	6	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7378	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\WERDD88.tmp.WERInternalMetadata.xml	7624	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7628	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7630	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\WERDD88.tmp.WERInternalMetadata.xml	7656	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7660	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7662	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 34 00 32 00 3a 00 35 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T05:42:50Z">	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7762	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7766	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	7770	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 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 31 00 35 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 33 00 35 00 39 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 33 00 35 00 39 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="417" PID="5156" UptimeMS="3593" TimeSinceCreationMS="3593" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8032	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8036	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\WERDD88.tmp.WERInternalMetadata.xml	8042	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 35 00 35 00 35 00 30 00 30 00 38 00 30 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="5550080" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8224	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8228	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8232	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\WERDD88.tmp.WERInternalMetadata.xml	8252	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8256	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8258	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
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8296	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8300	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8302	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\WERDD88.tmp.WERInternalMetadata.xml	8340	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8344	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8348	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 64 00 38 00 36 00 63 00 66 00 32 00 65 00 2d 00 37 00 32 00 35 00 34 00 2d 00 34 00 37 00 38 00 31 00 2d 00 62 00 33 00 30 00 38 00 2d 00 38 00 62 00 30 00 34 00 63 00 61 00 64 00 65 00 32 00 38 00 64 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>8d86cf2e-7254-4781-b308-8b04cade28d3</Guid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8446	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8450	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\WERDD88.tmp.WERInternalMetadata.xml	8454	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 34 00 32 00 3a 00 35 00 30 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-23T05:42:50Z</CreationTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8552	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8556	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8558	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\WERDD88.tmp.WERInternalMetadata.xml	8598	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD88.tmp.WERInternalMetadata.xml	8602	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
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE01A.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 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 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_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_077be6ee\Report.wer	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_077be6ee\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_W3X_e6deee335863428d576ebaa51f7a212f69d3e2_11952a33_077be6ee\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 32 00 39 00 32 00 37 00 38 00 32 00 35 00 30 00 38 00	MetadataHash=-292782508	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\{81e00543-02b3-baf3-c8d2-239b16bcdeb2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{81e00543-02b3-baf3-c8d2-239b16bcdeb2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{81e00543-02b3-baf3-c8d2-239b16bcdeb2}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA607EE3FE	unknown

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

Analysis Process: rundll32.exe PID: **6520**, Parent PID: **7148**

General

Target ID:	11
Start time:	22:42:49
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\W3XqCWvDWC.dll,DllRegisterServer
Imagebase:	0x7ff760ae0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
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	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6384**, Parent PID: **580**

General

Target ID:	15
Start time:	22:43:12
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: **6664**, Parent PID: **580**

General

Target ID:	16
Start time:	22:43:20
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: **6072**, Parent PID: **580**

General

Target ID:	17
Start time:	22:43:21
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: **6472**, Parent PID: **580**

General

Target ID:	19
Start time:	22:43:36
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: **5964**, Parent PID: **580**

General

Target ID:	25
Start time:	22:44:03
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: **4988**, Parent PID: **580**

General

Target ID:	27
Start time:	22:44:23
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

Analysis Process: svchost.exe PID: **6240**, Parent PID: **580**

General	
Target ID:	29
Start time:	22:44:33
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly