ID: 631906
Sample Name: W3XqCWvDWC
Cookbook: default.jbs
Time: 22:28:12
Date: 22/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

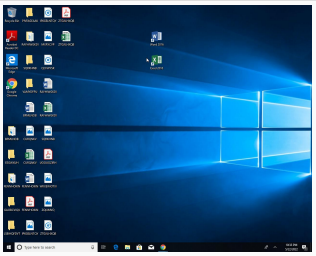
Windows Analysis Report

W3XqCWvDWC

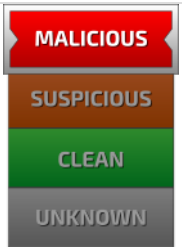
Overview

General Information

Sample Name:	W3XqCWvDWC (renamed file extension from none to dll)
Analysis ID:	631906
MD5:	661a35a77c5667..
SHA1:	81041189ebf61e..
SHA256:	1abc2d91d10d8a..
Tags:	exe trojan
Infos:	



Detection



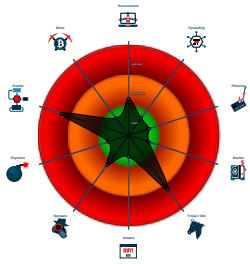
Emotet

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7136 cmdline: loaddll64.exe "C:\Users\user\Desktop\W3XqCWvDWC.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7152 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\W3XqCWvDWC.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5116 cmdline: rundll32.exe "C:\Users\user\Desktop\W3XqCWvDWC.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 6520 cmdline: C:\Windows\system32\WerFault.exe -u -p 5116 -s 336 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - regsvr32.exe (PID: 7164 cmdline: regsvr32.exe /s C:\Users\user\Desktop\W3XqCWvDWC.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6176 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KYnbMwv\FkmMqbieZ.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 3628 cmdline: rundll32.exe C:\Users\user\Desktop\W3XqCWvDWC.dll,AddIn_FileTime MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 6360 cmdline: C:\Windows\system32\WerFault.exe -u -p 3628 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 5852 cmdline: rundll32.exe C:\Users\user\Desktop\W3XqCWvDWC.dll,AddIn_SystemTime MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6532 cmdline: rundll32.exe C:\Users\user\Desktop\W3XqCWvDWC.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 4744 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 6440 cmdline: C:\Windows\system32\WerFault.exe -pss -s 428 -p 5116 -ip 5116 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - WerFault.exe (PID: 6468 cmdline: C:\Windows\system32\WerFault.exe -pss -s 492 -p 3628 -ip 3628 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- svchost.exe (PID: 1388 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5268 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4028 cmdline: c:\windows\system32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5832 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3264 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5528 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.385599828.0000021F07620000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.423121816.0000029D0DC80000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.422408365.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.385750200.0000029D0DC80000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.884802021.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.21f07620000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.29d0dc80000.2.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.0.rundll32.exe.21f07620000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.0.rundll32.exe.21f07620000.2.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.cf0000.0.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

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)

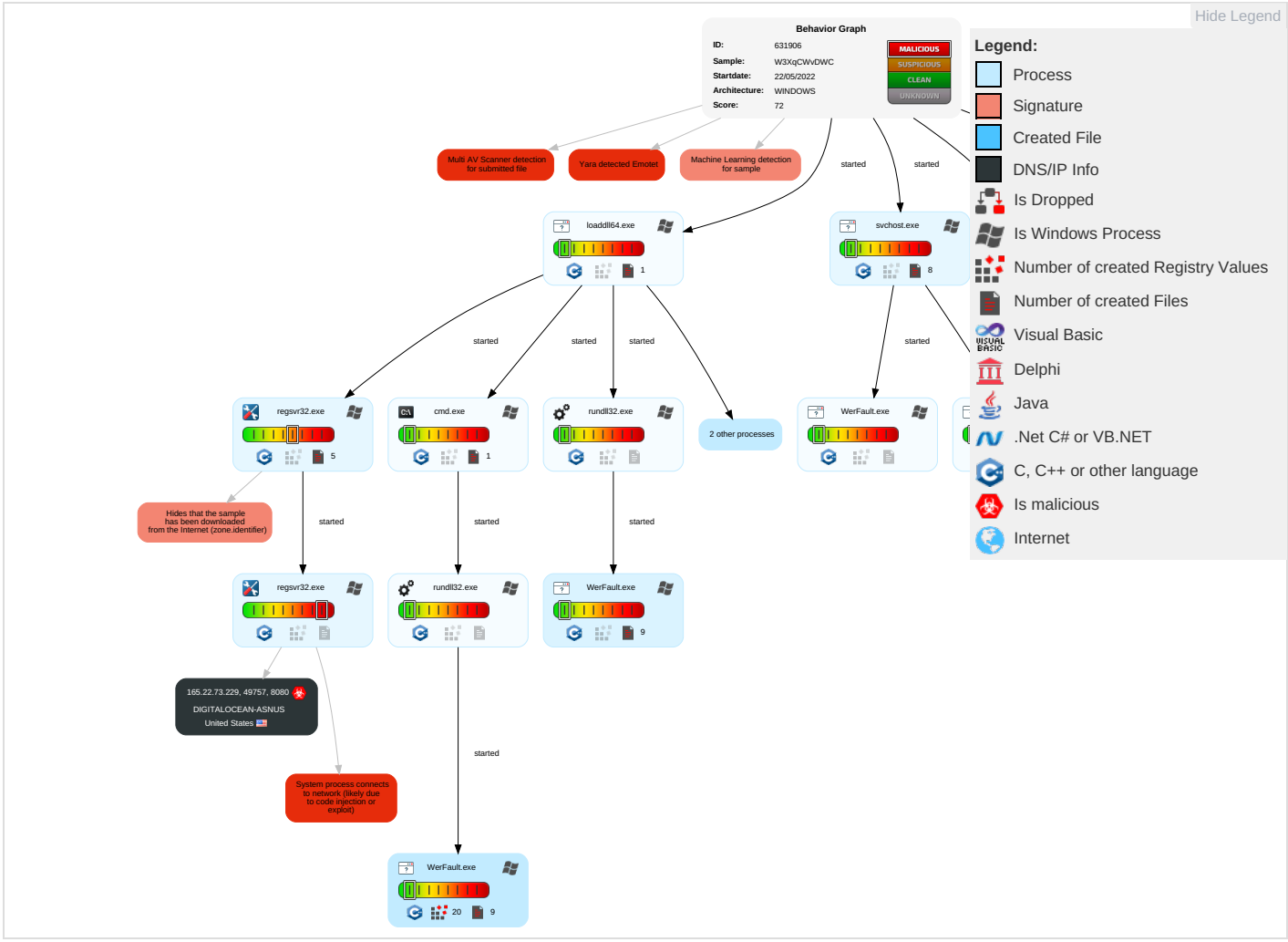
Stealing of Sensitive Information

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

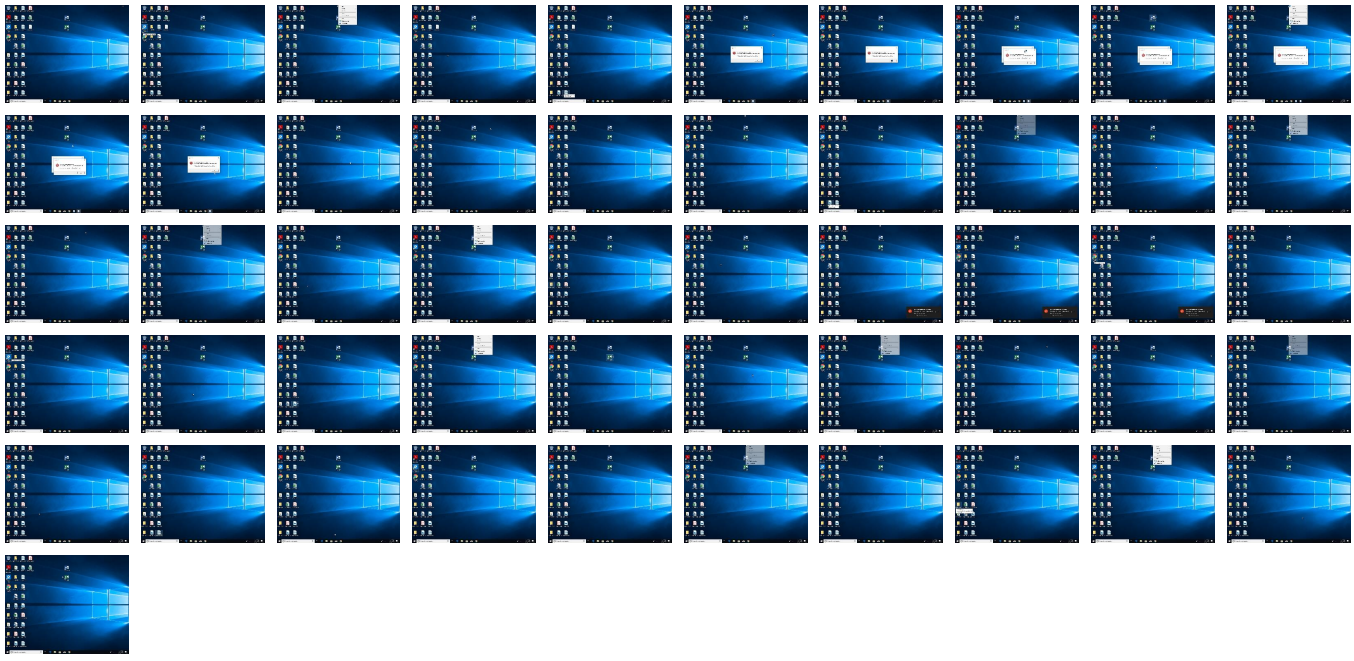
Behavior Graph



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	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
7.2.regsvr32.exe.1f20000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.29d0dc80000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.21f07620000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
2.2.regsvr32.exe.cf0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.0.rundll32.exe.29d0dc80000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
4.0.rundll32.exe.29d0dc80000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.21f07620000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.21f07620000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001D.00000003.699848849.000001F138F9E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001D.00000003.699848849.000001F138F9E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/	regsvr32.exe, 00000007.00000003.681201624.000000000065B000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.681285538.0000000000642000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.884301913.000000000062B000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.884354736.000000000065C000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.884330143.0000000000643000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.681151375.0000000000633000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001D.00000003.695210547.000001F139402000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.695235903.000001F138FA7000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.695226327.000001F138F96000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.695254149.000001F139402000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.pango.co/privacy	svchost.exe, 0000001D.00000003.695210547.000001F139402000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.695235903.000001F138FA7000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.695226327.000001F138F96000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.695254149.000001F139402000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001D.00000003.699848849.000001F138F9E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229/	regsvr32.exe, 00000007.00000003.681201624.000000000065B000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.884354736.000000000065C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://165.22.73.229:8080/temD	regsvr32.exe, 00000007.00000003.681285538.0000000000642000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.884330143.0000000000643000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.681151375.0000000000633000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ver)	svchost.exe, 00000019.00000002.885098836.00000194FAC00000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000002.726705919.000001F138F00000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001D.00000003.704245305.000001F139402000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.704223588.000001F138F9E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://help.disneyplus.com.	svchost.exe, 0000001D.00000003.699848849.000001F138F9E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressin	svchost.exe, 00000019.00000002.884582548.00000194F54AF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 0000001D.00000003.695210547.000001F139402000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.695235903.000001F138FA7000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.695226327.000001F138F96000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001D.00000003.695254149.000001F139402000.00000004.00000020.00020000.00000000.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: 22/05/202222:28:12	2022-05-22 22:28:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	W3XqCWvDWC (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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:	mal72.troj.evad.winDLL@32/16@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: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 13.89.179.12, 20.189.173.22, 173.222.108.210, 173.222.108.226, 93.184.221.240, 69.192.160.56, 20.223.24.244
- Excluded domains from analysis (whitelisted): onedsblobprdwus17.westus.cloudapp.azure.com, onedsblobprdcus17.centralus.cloudapp.azure.com, a767.dspw65.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu.azureedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, sls.update.microsoft.com, hlb.apr-52dd2-0.edgecastdns.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, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, neu-displaycatalogrp.useroor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.even
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: W3XqCWvDWC.dll

Simulations

Behavior and APIs

Time	Type	Description
22:29:56	API Interceptor	2x Sleep call for process: WerFault.exe modified
22:31:07	API Interceptor	10x 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\qmgr.db

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xd1c7ce56, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25074921083906204
Encrypted:	false
SSDEEP:	384:U+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:rSB2nSB2RSjlK/+mLesOj1J2
MD5:	655EF77631B804E811F945211D0860EC
SHA1:	15878DB9A86EDB93C7FC9D382E3298F69A914105
SHA-256:	406019DA88D19D1184B21C19CB8E0B0B928BB9E9092DD2557368BD08A48ACADB
SHA-512:	D8302FE347B93AC0E11397930015B9D6BA09EF8EAD51FD5FE5D64ED6548A820FD2DAA13CA9E3F8B8A7B2A7EAB5925AF97060F4927D043078DC3E5B5D071F44D0
Malicious:	false
Preview:	...V... .....e.f.3...w.....&.....w.....z..h.(.....3...w.....B.....@..... ....3...w..... .....V.....z.....?.....z..... .....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_188de68a\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):	0.7861290894240726
Encrypted:	false
SSDEEP:	96:qDF9UivJPnySjv55od7Rt6tpXIQcQac6FcEocw3ZXaXz+HbHgSQgJPbwqIDV9w8j:MMivJKgHkBy9jJ9/u7sYS274lt+I
MD5:	93245C6EC22D32CE8F51441732DEF5C0
SHA1:	754BD6C0F4767B3DE819B860F0938DAAF865FB81
SHA-256:	04F12EC43F8F211B0CC6E02860BFD7ED7C3414860EA480A3A0A43F7A47EF5D72
SHA-512:	F6C7FCC1997E5179AED4FE4763CFDF5496CB19CEF90281F33CCB1C10757718BDAD42D3FAACEF64D77E2986EBF883B3568DCDA64DAD5964956D8054FC8C4EB81
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.6.4.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.7.5.7.3.8.9.1.8.3.6.4.8.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.5.7.3.9.5.0.8.9.8.5.1.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.a.5.4.8.0.8.3.-.4.b.3.e.-.4.5.0.e.-.9.2.1.2.-.7.2.9.1.0.a.9.e.f.8.8.4...I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.f.d.2.2.1.7.b.-.1.0.3.3.-.4.b.5.d.-.8.3.3.6.-.9.3.c.5.6.d.c.4.8.b.f.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.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.=.0.0.0.0.0.e.2.c.-.0.0.0.1.-.0.0.1.8.-.b.e.2.b.-.1.9.1.4.6.6.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_192de409\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):	0.785280213024148
Encrypted:	false
SSDEEP:	96:18F6YcFUiD2JPnyLjv55od7Rt6tpXIQcQac6FcEocw3ZXaXz+HbHgSQgJPbwqIDP:i//iD2JKhHkBy9jJ9/u7sYS274lt+I
MD5:	80B2294DA5AA05766AB50AA915D7891E
SHA1:	F6E866D499EF299403F071710D3AC41DC9251588
SHA-256:	FC36EA83A7AF34E6CA9FE238A523AE2060AF9D16200F8FE87F291A0159E877BC
SHA-512:	2636F604D6C4B1F908C93F6378C17332A8C389DF85EC7FAB1CF55F2C9017636C64865FC40B913AA3FBFAA8B55D9858D56FF28EDE54094FB2042FD3B93291E9D
Malicious:	false

Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.6.4.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.7.5.7.3.8.8.0.3.8.5.1.3.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.5.7.3.9.4.4.9.1.5.9.0.1.....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.=.c.4.6.6.5.7.9.3.-.d.0.c.9.-.4.9.b.0.-.a.2.a.f.-.7.e.9.0.c.c.3.c.e.7.c.c... ..I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.f.b.c.b.1.6.b.-.6.8.4.9.-.4.7.7.b.-.b.f.c.4.-.2.b.9.9.2.2.1.5.d.d.1.c.....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.=.0.0.0.0.1.3.f.c.-.0.0.0.1.-.0.0.1.8.-.a.3.b.f.-.9.a.1.3.6.6.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 05:29:49 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	62524
Entropy (8bit):	2.368950805352583
Encrypted:	false
SSDEEP:	384:MA04cSe2YqH2jC2s4V3kMcldYncnfD5zJ+3y:pfMqH2jCj4xz+RfDrKy
MD5:	DA3AB356F2B46AAD9C8F0FDF9E53B268
SHA1:	2454B3D70D79519F53CCB060D13A111491AEF099
SHA-256:	B8A8C6BF0E4777E5DA3BC1291C38FAC4976EEFD888964C5E9F28D2C269D19946
SHA-512:	4595A8F4080186B5E243A5B1179C62A4DA64C1F6A6D0BE9625C96229B4F6F479C43761900667A6F926829C1D0DB7A7B1DC279A52561D94F68ECFA438D977FD54
Malicious:	false
Preview:	MDMP..... .....b.....8.....$...d;.....`.....8.....T.....".....$.....U.....B.....P%... ...Lw.....Y...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\WERC844.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 05:29:50 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.27560589422894
Encrypted:	false
SSDEEP:	192:aV4ISFa04cqPyowuCSrMV/qkm+s494cuBOC5Ic6wHXdOYXqf1XItVSqv7awII+mf:YL04cSe2YqH2pC2crcldYnYTlG
MD5:	40723BED99C639BDBCECCB9C93712EA7
SHA1:	04DDBEAFF0D58083313E19E289E7FEDEDBB8D551
SHA-256:	09DF41903027B5537B9E65985974A84C93B4C782A58393490F33D671EE61F353
SHA-512:	683FB76E4342B3DE71016F3644304C4A301568797A27335E4CEAAB539E0328634B372EEBCC33D1C5FF1605BEC9EA716C06EAB6CE74A39877293062A10FF19E14
Malicious:	false
Preview:	MDMP..... .....b.....8.....$...d;.....`.....8.....T.....X.....".....$.....U.....B.....P%... ...Lw.....T.....,.....b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8654
Entropy (8bit):	3.6977082844769855
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNimCRH+PzA6YqjCgmf8uSkCprf89b/xKfmZVm:RrlsNiTRH+bA6YuCgmf8uS8/8fN
MD5:	C5846E0BCC037A8A65264DCC3278F594
SHA1:	8DEF6CCCE22677DBBD4571919477854C8905F420
SHA-256:	31A25ECBB877C672C188FB63C59AEBB7CB5625C096DB9857AE1E6A546F49F3C5
SHA-512:	D20553FACFD18FBF1A20A408FBFCB15CFF8AA64D50BFFF19C2F9349235C4BA3E266B0E03109A1D36EAE0EA5FB718CF5F0C182268A5218B23BC68513B599903 D
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.>.5.1.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0C2.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):	4.508316787911904
Encrypted:	false
SSDEEP:	48:cvIwSD8zsXJgtBI9fnWgc8sqYjmFa8fm8M4JCqC9fwnF4Fyq8vh9fwV0ZESC5SLd:uITf55WgrsqYCRJ2FWFVvLd
MD5:	AFBA7F16C9005E8C855248ABC1D2F8CD
SHA1:	CE060E98EE3A5807B6316DCC05210D78F33A59EF
SHA-256:	5ECE0E0F46041834E4A5F9184FF89B53D88161276839AB42C38FC5C8ACCCD403
SHA-512:	F59A3E961A3B405B3258C2F533F0C7E520845BABC23230FD484504C6951CB262F00AEB5DEBDEBC26620826F3435E7C4CC34DFB866FF39BB190B3A8347E4F9E9F
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1527280" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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):	6862
Entropy (8bit):	3.7235885574018686
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiiCQfc+xuY8uSkCpri89b2U+feSm:RrlsNiYfc+xuY8uSH2Nfy
MD5:	3599DA8B34D1693CE09BD96799977A41
SHA1:	9E9B79CCC5FFA070DFDEF7C8F82F7B67B64C2E05
SHA-256:	B6E677966A3FF82F0EF52B40578E7F18D872732AC1B82F2522267F151DC9641C
SHA-512:	0D50A17C725B44E5AAC5E57B871EF6DCD1C8BF6156719BA55498D4DBB39C80F6F092510F2BED680342C47CC428F333B82DCBAEF8BF011FF55EE744792389608E
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.6.2.8.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD544.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54318
Entropy (8bit):	3.0561636569688413
Encrypted:	false
SSDEEP:	1536:9bHI2UZ/nfGgSu40/v9BiWf/0xk29kAuy6KyM:9bHI2UZ/nfGgSu4039BiWf/0xk29kAuk
MD5:	C16FA7D7DD76E81D9F75A377422A40E5
SHA1:	CC322D768197C5E65010DC6AB51C4675A3180879
SHA-256:	133C390D6338F019FA3DED9D1BED7601C0566569D371ADA0DBD6EEF262288BE1
SHA-512:	7308C35D649F0B2F3896338482B4DFCC21DB3B98698FB802663EC6E1D5AEEB9FCE0B26D02CB4307F34AF256399D5A2FFE09205B0AF757D73209FE5FE604086C
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD882.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):	4.508597638922555
Encrypted:	false
SSDEEP:	48:cvIwSD8zsXJgtBI9fnWgc8sqYjf8fm8M4JCqC9fwnFRIUyq8vh9fwW0ZESC5SAd:uITf55WgrsqYgJ3pW4VvAd
MD5:	D0FC83B05EB92CE4D87C84057BE2B115
SHA1:	D61BD274F91D89C5258086D8D0EEBDC1DEEE927F
SHA-256:	6E0D93A6FA8AF71EA7A89934F69C64FFDF63954F6E3A9835EEFC2A64B127A1D7
SHA-512:	6744B25A44AA3F4393ED56D5CB2919516467C588B41EF90D02BDE321A90B66F27B212104CDA5CDB70B2D961E94D6A5ADA8FF6906604AA3C6DE597F618DDBAE1A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1527280" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERD95C.tmp.csv

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	54334
Entropy (8bit):	3.056249879577972
Encrypted:	false
SSDEEP:	1536:2CHPIOQnfiTu40/vYoYWf/sxt8JqAuVH2yD:2CHPIOQnfiTu403YoYWf/sxt8JqAuVHf
MD5:	4ED04F837989BC6C4C2B298FAE9D6B8D
SHA1:	EE7BBDA8D2E7DC62055926CF23DC8BD1487C5BB7
SHA-256:	86527C3AB8041506EFB5934F542D4ED464CFBABABD67C23491D4EC535739DA15
SHA-512:	53CE10FDED9BE6FCCE86D5ED524EC0FE44F3578CCF58C58FDCCFA6C1F32B90EA0F9B162FBD87DC62BE3CC42954AA4182C81868E1E59B9BC698589C5221E0B1F
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA57.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.697454980773062
Encrypted:	false
SSDEEP:	96:kiZYWXl+2ohmYQYUWoNHqYEZ4Mt8iKLOf8ywlkwa+EJ/SIIf23:hZDXl/H952Za+EJ/Svf23
MD5:	641B834246796078E459F1290191AF59
SHA1:	F326AD099635D3F0B95513EE82C4E7DB14B6A6EB
SHA-256:	A3A5222E604078C7CADA19AAFF53D4AF81354C7DB9FAC48149D0F7B883D4330D
SHA-512:	68A6F05D9B66A2659345CAAB9DD0805A72338B29280D76A577B615FE1ABDAB5A36D2E0BE9A160B288897DB4DD66F9BF3029AC026691BD22322D7184138B9C082
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD17.tmp.txt

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.697780492905745
Encrypted:	false
SSDEEP:	96:kiZYWGjZLRXYoYyWQHqYEZ8Nt8iKLOk8ywm1izLazEqGSIIB23:hZD2PhS4zLazEqGSvB23
MD5:	D63DD4C4EA9E1107F0D97535D2829F7F
SHA1:	7486551A9A93294C1B76A467C7DC46102792CD1F
SHA-256:	31AEE2D8CB178F469BDB1507972D8F4B3881DF1DB6EBB86B1ABA5CB6B6598174
SHA-512:	57CC8814B7DEB16EFED8440A7DF9FA888F21276E346FC207B9A46AB76844197895B42407DFD6E509F77C90FA9AF856A598241391DC5A95641200BC990A3AE18D
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.2.6.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB16994 76
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27...._...+).lE..he.4|.?,...h....7..PA..b,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A...  ....I_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:`:.....  ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`.....`._.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...l.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.....I...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	330
Entropy (8bit):	3.120848828934212
Encrypted:	false
SSDEEP:	6:kK5ooJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:BakPlE99SNxAhUesE1
MD5:	603C5F0CEFFCB07D2BC7E3B0921C6F69
SHA1:	FC148E38295C25F1BF82E1E17A6C6ECD40496293
SHA-256:	D8D2F8840CB2F29FCEFFF4A572756C4D212872DAA04332629187833D28CDAC1D
SHA-512:	29EFA296659770BDC21A4A3325E03345E75D59ED906730D5236853C3770896D9F9C67F54DC0922B14F29E90DD3FC29E7E016458B83461EA9BDE86DBC9D3D3E9
Malicious:	false
Preview:	p..... .....K+fn..(..... .....3k/"[.....(.....(...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

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

Instruction
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 00007FB938BBE1C7h
call 00007FB938BC3527h
dec esp
mov eax, dword ptr [esp+40h]
mov edx, dword ptr [esp+38h]
dec eax
mov ecx, dword ptr [esp+30h]
call 00007FB938BBE1D4h
dec eax
add esp, 28h
ret
int3
int3
int3
int3
int3
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 00007FB938BBE1D2h
cmp dword ptr [00028DE8h], 00000000h
jne 00007FB938BBE1C9h
xor eax, eax
jmp 00007FB938BBE2E4h
cmp dword ptr [esp+58h], 01h
je 00007FB938BBE1C9h
cmp dword ptr [esp+58h], 02h
jne 00007FB938BBE210h
dec eax
cmp dword ptr [0001ED99h], 00000000h
je 00007FB938BBE1DAh
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 00007FB938BBE1D9h
dec esp

Instruction
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call 00007FB938BBDF2Ah
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
jne 00007FB938BBE1C9h
xor eax, eax

Rich Headers

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

Data Directories

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

Name	RVA	Size	Type	Language	Country

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

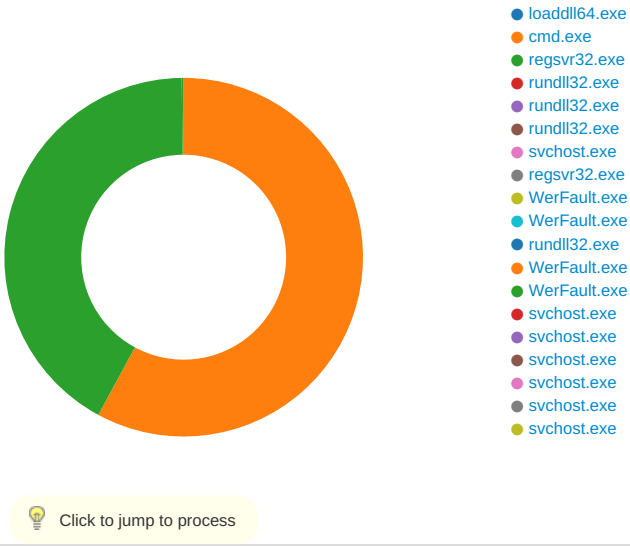
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 22:30:09.205770016 CEST	49757	8080	192.168.2.7	165.22.73.229
May 22, 2022 22:30:09.248379946 CEST	8080	49757	165.22.73.229	192.168.2.7
May 22, 2022 22:30:09.248512030 CEST	49757	8080	192.168.2.7	165.22.73.229
May 22, 2022 22:30:09.315850973 CEST	49757	8080	192.168.2.7	165.22.73.229
May 22, 2022 22:30:09.358282089 CEST	8080	49757	165.22.73.229	192.168.2.7
May 22, 2022 22:30:09.368135929 CEST	8080	49757	165.22.73.229	192.168.2.7
May 22, 2022 22:30:09.368191957 CEST	8080	49757	165.22.73.229	192.168.2.7
May 22, 2022 22:30:09.368587017 CEST	49757	8080	192.168.2.7	165.22.73.229
May 22, 2022 22:30:12.461575031 CEST	49757	8080	192.168.2.7	165.22.73.229
May 22, 2022 22:30:12.505445957 CEST	8080	49757	165.22.73.229	192.168.2.7
May 22, 2022 22:30:12.505577087 CEST	49757	8080	192.168.2.7	165.22.73.229
May 22, 2022 22:30:12.512813091 CEST	49757	8080	192.168.2.7	165.22.73.229
May 22, 2022 22:30:12.596580982 CEST	8080	49757	165.22.73.229	192.168.2.7
May 22, 2022 22:30:12.764410019 CEST	8080	49757	165.22.73.229	192.168.2.7
May 22, 2022 22:30:12.764496088 CEST	49757	8080	192.168.2.7	165.22.73.229
May 22, 2022 22:30:15.768646002 CEST	8080	49757	165.22.73.229	192.168.2.7
May 22, 2022 22:30:15.768675089 CEST	8080	49757	165.22.73.229	192.168.2.7
May 22, 2022 22:30:15.768793106 CEST	49757	8080	192.168.2.7	165.22.73.229
May 22, 2022 22:31:59.324021101 CEST	49757	8080	192.168.2.7	165.22.73.229

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 22:31:59.324043989 CEST	49757	8080	192.168.2.7	165.22.73.229

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **7136**, Parent PID: **1524**

General

Target ID:	0
Start time:	22:29:28
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:	0x7ff77d910000
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: **7152**, Parent PID: **7136**

General

Target ID:	1
Start time:	22:29:29
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:	0x7ff6a6590000
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: 7164, Parent PID: 7136

General

Target ID:	2
Start time:	22:29:30
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:	0x7ff799140000
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: 00000002.00000002.383775836.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.383431733.0000000000CF0000.00000040.00001000.00020000.00000000.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\KYnbMwv\FkmMqbieZ.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: 5116, Parent PID: 7152

General

Target ID:	3
Start time:	22:29:30
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:	0x7ff728e80000
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: 00000003.00000000.385599828.0000021F07620000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.420849209.0000021F07620000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.385379226.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.383190699.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.383957079.0000021F07620000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.420695494.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **3628**, Parent PID: **7136**

General

Target ID:	4
Start time:	22:29:31
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:	0x7ff728e80000
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: 00000004.00000002.423121816.0000029D0DC80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.422408365.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.385750200.0000029D0DC80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.384165191.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.385421793.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.384837851.0000029D0DC80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **5852**, Parent PID: **7136**

General

Target ID:	5
Start time:	22:29:37
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:	0x7ff728e80000
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: svchost.exe PID: **4744**, Parent PID: **604**

General

Target ID:	6
Start time:	22:29:37
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff7e8070000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
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

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **6176**, Parent PID: **7164**

General

Target ID:	7
Start time:	22:29:38
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\KYnbMwv\FkmMqbieZ.dll"
Imagebase:	0x7ff799140000
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: 00000007.00000002.884802021.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.884543740.0000000001F20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **6440**, Parent PID: **4744**

General

Target ID:	8
Start time:	22:29:38
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -pss -s 428 -p 5116 -ip 5116
Imagebase:	0x7ff7e8070000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **6468**, Parent PID: **4744**

General

Target ID:	9
Start time:	22:29:38
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -pss -s 492 -p 3628 -ip 3628
Imagebase:	0x7ff684030000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: **6532**, Parent PID: **7136**

General

Target ID:	10
Start time:	22:29:40
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:	0x7ff728e80000
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: WerFault.exe PID: **6520**, Parent PID: **5116**

General

Target ID:	11
Start time:	22:29:42
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 5116 -s 336
Imagebase:	0x7ff684030000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8BB61527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0C2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0C2.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_192de409	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_192de409\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0C2.tmp	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0C2.tmp.xml	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD544.tmp.csv	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDA57.tmp.txt	success or wait	1	7FF8BB60E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 1b fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.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 fd fd 59 02 00 00 54 05 00 00 fd 03 00 00 fd 13 00 00 fd 1b fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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%LwYTb0Pacific Standard TimePacific Daylight Time	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	10276	1232	fd 39 fd 05 1f 02 00 00 7d 45 2e fd fd 7f 00 00 00 00 fd 28 fd 7f 00 00 fd 0b 6a 07 1f 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 06 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 fd 1d fd 6e 00 00 00 00 fd 28 fd 7f 00 00 00 00 fd 28 fd 7f 00 00 00 00 fd 28 fd 7f 00 00 58 fd 56 45 fd 00 00 00 fd fd 56 45 fd 00 00 00 fd 03 03 00 00 00 00 00 28 fd 56 45 fd 00 00 00 4c 53 fd 05 1f 02 00 00 0a 00 00 00 00 00 00 00 28 02 fd 17 fd 0f 00 00 fd fd fd fd fd fd fd fd 52 fd 05 1f 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 0a fd 05 1f 02 00 00 fd 00 00 00 00 00 00	9}E.(j_3++S++ (n(((XVEVE(VELS(R(	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	1632	168	10 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 00 00 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	15204	20	52 00 00 00 00 60 67 45 fd 00 00 00 fd 07 00 00 fd 40 00 00	R`gE@	success or wait	82	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	16520	1976	00 00 00 04 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 fd 28 fd 7f 00 00 60 fd fd fd fd 7f 00 00 60 1c fd 05 1f 02 00 00 00 00 00 00 00 00 00 00 00 00 fd 05 1f 02 00 00 fd fd fd fd 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 70 30 35 fd fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 fd 05 1f 02 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd 7f 00 00 fd 03 01 00 00 00 00 00 00 00 34 fd fd 7d 00 00 00 00 00 00 00 00 00 00 30 07 34 fd fd 7d 00 00 00 00 47 fd fd 7d 00 00 28 02 48 fd fd 7d 00 00 50 06 49 fd fd 7d 00 00 04 00 00 00 00 00 00 00 00 fd fd 07 6d fd fd fd 00 00 10 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 10 00 00 00 00 00 00 05 00 00 00 10 00 00 00 20 fd fd fd fd 7f 00 00 00 00 fd 05 1f 02 00	(``p054}04}G}(H}PI}m	success or wait	81	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	56244	936	76 fd fd fd fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 fd fd fd 7f 00 00 10 00 00 00 00 00 00 00 fd fd 5e 45 fd 00 00 00 fd fd 5e 45 fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 60 67 45 fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 30 4b fd 05 1f 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 fd 30 fd 05 1f 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5c 00 00 00 00 00 00 00 5c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	v`2^E^E`gE0K0\\	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	11508	1232	68 fd 56 45 fd 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 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 78 fd 56 45 fd 00 00 00 fd fd fd fd fd fd fd fd 78 fd 56 45 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 56 45 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 78 fd 56 45 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 7f 00	hVE 3++S++FxVExVEVExVE	success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	1900	48	14 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 67 45 fd 00 00 00 58 fd fd 45 fd 00 00 00 fd 07 00 00 54 fd 00 00 fd 04 00 00 fd 36 00 00	gEXET6	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	4556	4344	00 00 fd fd 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 fd fd 7f 00 00 fd fd fd fd 7f 00 00 00 00 03 fd 01 00 00 00 fd 7b 74 17 66 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 01 00 00 00 00 00	<2|h+(BB?#`A pS{tfnS	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.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 fd fd 02 00 00 00 00 00 fd 0b 03 00 00 00 00 1f 0e 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 7d fd 03 00 00 00 00 00 65 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 52 fd 1a 00 00 00 00 00 fd 5f 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 04 2b 06 00 00 00 00 00 10 11 fd 71 00 00 00 00 7a 1c 3f 1e 00 00 00 00 fd fd fd 20 00 00 00 00 fd 25 1f 01 00 00 00 00 fd 03 01 00 fd 10 01 00 fd fd 05 00 fd 58 0a 00 fd 5f 05 00 06 7f 15 00 04 2b 06 00 fd fd 39 00 fd fd 01 00 fd 6f 15 00 00 00 00 fd fd 25 00 fd 63 04 00 b9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6f 02 00	Zb}R_@+qz? %X_+9o%co	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	57180	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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC3CF.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 fd 10 00 00 38 12 00 00 05 00 00 00 24 05 00 00 64 3b 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	8$d;`8T"$	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 31 00 31 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5116</Pid>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 34 00 34 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20442</Uptime>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1230	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404"> 0</Wow64>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1430	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 35 00 30 00 33 00 38 00 30 00 34 00 34 00 31 00 36 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>2203503804416 </PeakVirtualSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1536	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 34 00 30 00 38 00 31 00 37 00 31 00 30 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203408171008</VirtualSize>	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1626	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 32 00 39 00 35 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>26295</PageFaultCount>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1712	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 32 00 31 00 34 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>105021440</PeakWorkingSetSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1822	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 36 00 39 00 36 00 39 00 36 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>7069696</WorkingSetSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	1912	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>106776</QuotaPeakPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2036	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>106576</QuotaPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2144	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21504</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2278	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21152</QuotaNonPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2396	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 33 00 35 00 30 00 30 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1835008</PagefileUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2482	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 34 00 36 00 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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2588	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 33 00 35 00 30 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1835008</PrivateUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2668	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2722	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2752	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2756	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2762	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2802	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2806	2	09 00		success or wait	4	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2814	30	3c 00 50 00 69 00 64 00 3e 00 37 00 31 00 35 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7152</Pid>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2844	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2848	2	09 00		success or wait	4	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2856	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2916	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2920	2	09 00		success or wait	4	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	2928	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3018	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3022	2	09 00		success or wait	4	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3030	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 31 00 33 00 34 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>21345</Uptime>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3086	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3176	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3240	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3298	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203370262528</PeakVirtualSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3408	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203370262528</VirtualSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3502	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 39 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>794</PageFaultCount>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3588	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 39 00 32 00 30 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2920448</PeakWorkingSetSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3684	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3688	2	09 00		success or wait	5	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3698	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 38 00 30 00 31 00 36 00 36 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>28016 64</WorkingSetSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3792	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>27840 </QuotaPeakPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	3918	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >27664</Qu otaPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4014	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4018	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4028	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>42 08</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4164	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>3664</QuotaNonPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4284	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 39 00 38 00 32 00 37 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>2998272</PagefileUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4360	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4364	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4374	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 34 00 35 00 37 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3145728</PeakPagefileUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4480	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 39 00 38 00 32 00 37 00 32 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2998272</PrivateUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4564	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4620	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4670	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4708	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4756	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4802	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX64</EventType>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4858	4	0d 00 0a 00		success or wait	9	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4862	2	09 00		success or wait	18	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	4866	104	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	5652	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	5656	2	09 00		success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	5658	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	5698	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	5702	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	5704	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	5742	4	0d 00 0a 00		success or wait	6	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	5746	2	09 00		success or wait	12	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	5750	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6304	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6308	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6310	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6350	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6354	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6356	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6402	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6496	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6500	2	09 00		success or wait	2	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6504	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 65 00 6c 00 79 00 6d 00 79 00 6c 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>elymyl, Inc.</SystemManufacturer>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6610	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6614	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6618	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 6c 00 79 00 6d 00 79 00 6c 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>elymyl7,1</SystemProductName>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6714	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6718	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6722	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6842	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6846	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6850	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 37 00 34 00 30 00 30 00 30 00 34 00 33 00 36 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>1617400436</OSInstallDate>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6932	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6936	2	09 00		success or wait	2	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	6940	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7042	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7046	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7050	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7118	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7122	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7124	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7164	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7168	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7170	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7212	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7308	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7312	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7314	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7350	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7354	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7356	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7380	4	0d 00 0a 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7384	2	09 00		success or wait	6	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7388	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7634	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7638	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7640	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7666	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7670	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7672	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 35 00 30 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T05:29:50Z">	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7772	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7776	2	09 00		success or wait	2	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	7780	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 31 00 31 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 36 00 35 00 33 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 35 00 33 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="406" PID="5116" UptimeMS="6531" TimeSinceCreationMS="6531" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8052	184	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 35 00 34 00 33 00 39 00 34 00 38 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5439488" TimelineUnitShift="12" Timeline="1111"/>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8236	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8240	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8244	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8264	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8268	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8270	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8308	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8312	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8314	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8352	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8356	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8360	98	3c 00 47 00 75 00 69 00 64 00 3e 00 63 00 34 00 36 00 36 00 35 00 37 00 39 00 33 00 2d 00 64 00 30 00 63 00 39 00 2d 00 34 00 39 00 62 00 30 00 2d 00 61 00 32 00 61 00 66 00 2d 00 37 00 65 00 39 00 30 00 63 00 63 00 33 00 63 00 65 00 37 00 63 00 63 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>c4665793-d0c9-49b0-a2af-7e90cc3ce7cc</Guid>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8458	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8462	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8466	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 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>2022-05-23T05:29:50Z</CreationTime>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8564	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8568	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8570	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8610	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCDD3.tmp.WERInternalMetadata.xml	8614	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD0C2.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_192de409\Report.wer	0	2	fd fd		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_192de409\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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_192de409\Report.wer	9590	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 32 00 32 00 38 00 30 00 37 00 38 00 37 00 39 00 32 00	MetadataHash=1228078792	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: WerFault.exe PID: **6360**, Parent PID: **3628**

General

Target ID:	12
Start time:	22:29:42
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3628 -s 328
Imagebase:	0x7ff684030000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF8BB61527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD882.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD882.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_188de68a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_188de68a\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8BB60E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD882.tmp	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD882.tmp.xml	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD95C.tmp.csv	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERDD17.tmp.txt	success or wait	1	7FF8BB60E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd 1b fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.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 18 fd fd 01 00 00 54 05 00 00 fd 03 00 00 2c 0e 00 00 fd 1b fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBP%LwT,b0Pacific Standard TimePacific Daylight Time	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	10276	1232	fd 03 02 00 00 00 00 00 fd 0b 04 0e fd 02 00 00 00 00 fd 28 fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 02 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 41 34 fd 6e 00 00 00 00 fd 28 fd 7f 00 00 00 00 fd 28 fd 7f 00 00 00 00 fd 28 fd 7f 00 00 08 fd fd 29 fd 00 00 00 fd fd fd 29 fd 00 00 00 fd 03 02 00 00 00 00 00 fd fd fd 29 fd 00 00 00 fd 5b 3b 0c fd 02 00 00 0a 00 00 00 00 00 00 00 28 02 fd 17 fd 0f 00 00 fd fd fd fd fd fd fd fd 40 5b 3b 0c fd 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 22 3c 0c fd 02 00 00 fd 00 00 00 00 00 00	(_3++S++A4n((()))[;(@[;" <	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	1632	168	44 0a 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	D$(	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	15204	20	52 00 00 00 00 fd 02 fd 01 00 00 00 06 00 00 00 fd 40 00 00	R@	success or wait	82	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	16520	6	01 04 01 00 04 22	"	success or wait	81	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	57636	2664	76 fd fd fd fd 7f 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 10 00 00 00 00 00 00 00 fd fd fd 29 fd 00 00 00 fd fd fd 29 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 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 60 fd 29 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 3b 0c fd 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 18 30 3b 0c fd 02 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 00 00 00 00 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	v))`);0;DD	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	11508	1232	00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 38 fd fd 29 fd 00 00 00 fd fd fd fd fd fd fd 38 fd fd 29 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd 29 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 38 fd fd 29 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 7f 00	3++S++F8)8))8)	success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	1900	48	fd 01 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd fd 29 fd 00 00 00 28 fd 07 2a fd 00 00 00 fd 08 00 00 fd 4a 00 00 fd 04 00 00 fd 36 00 00	)(*J6	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.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	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	4556	4344	00 00 fd fd 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 fd fd 7f 00 00 fd fd fd fd 7f 00 00 00 00 03 fd 01 00 00 00 fd 13 18 66 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 01 00 00 00 00 00	<2|h+(BB?#`A pSfnS	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.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 fd fd 02 00 00 00 00 00 fd 0b 03 00 00 00 00 30 0e 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 68 fd 03 00 00 00 00 00 65 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 1a 00 00 00 00 00 fd 4b 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 04 2b 06 00 00 00 00 00 10 11 fd 71 00 00 00 00 30 fd 44 1e 00 00 00 00 42 47 fd 20 00 00 00 00 3f fd 1f 01 00 00 00 00 fd 03 01 00 09 14 01 00 0a fd 05 00 fd 6f 0a 00 fd 4b 05 00 06 7f 15 00 04 2b 06 00 5c 49 3b 00 76 01 00 fd fd 15 00 00 00 00 00 fd 11 27 00 09 64 04 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6f 02 00	Zb0hK@+q0DBG ? oK+\I;'do	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	60300	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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC844.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 fd 10 00 00 38 12 00 00 05 00 00 00 24 05 00 00 64 3b 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 58 0d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	8$d;`8TX"$	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3628</Pid>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 32 00 30 00 35 00 35 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>20555</Uptime>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1230	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1430	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 35 00 30 00 33 00 38 00 32 00 30 00 38 00 30 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 03820800 </PeakVirtualSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1536	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 34 00 30 00 38 00 31 00 37 00 31 00 30 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>220340817 1008</VirtualSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1626	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 32 00 39 00 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>26296 </PageFaultCount>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1712	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 32 00 39 00 36 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>105029632</PeakWorkingSetSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1822	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 34 00 39 00 32 00 31 00 36 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>7049216</WorkingSetSize>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	1912	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>106776</QuotaPeakPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2036	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>106576</QuotaPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2144	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 36 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21632</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2278	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 32 00 38 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>21280</QuotaNonPagedPoolUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2396	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 37 00 32 00 39 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>1847296</PagefileUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2482	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 34 00 37 00 30 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101470208</PeakPagefileUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2588	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 34 00 37 00 32 00 39 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>1847296</PrivateUsage>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2668	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2720	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2762	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2766	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2768	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2806	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2810	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2814	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX64</EventType>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2870	4	0d 00 0a 00		success or wait	9	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2874	2	09 00		success or wait	18	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	2878	104	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	3664	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	3668	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	3670	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	3710	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	3714	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	3716	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	3754	4	0d 00 0a 00		success or wait	6	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	3758	2	09 00		success or wait	12	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	3762	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4316	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4320	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4322	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4362	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4366	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4368	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4406	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4410	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4414	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4508	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4512	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4516	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 65 00 6c 00 79 00 6d 00 79 00 6c 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>elymyl, Inc.</SystemManufacturer>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4622	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4626	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4630	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 65 00 6c 00 79 00 6d 00 79 00 6c 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>elymyl7,1</SystemProductName>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4726	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4730	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4734	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4862	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 37 00 34 00 30 00 30 00 30 00 34 00 33 00 36 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>1617400436</OSInstallDate>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4944	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4948	2	09 00		success or wait	2	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	4952	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5054	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5058	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5062	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5130	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5134	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5136	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5176	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5180	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5182	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5216	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5220	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5224	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5320	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5324	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5326	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5362	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5366	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5368	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5392	4	0d 00 0a 00		success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5396	2	09 00		success or wait	6	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5400	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5646	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5650	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5652	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5678	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5682	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5684	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 35 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T05:29:51Z">	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5784	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5788	2	09 00		success or wait	2	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	5792	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 30 00 37 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 36 00 32 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 37 00 36 00 30 00 39 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 37 00 36 00 30 00 39 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="407" PID="3628" UptimeMS="7609" TimeSinceCreationMS="7609" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6054	4	0d 00 0a 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6058	2	09 00		success or wait	6	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6064	184	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 35 00 34 00 34 00 33 00 35 00 38 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5443584" TimelineUnitShift="12" Timeline="1111"/>	success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6444	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6448	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6452	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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6472	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6476	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6478	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	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6516	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6520	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6522	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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6560	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6564	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6568	98	3c 00 47 00 75 00 69 00 64 00 3e 00 36 00 61 00 35 00 34 00 38 00 30 00 38 00 33 00 2d 00 34 00 62 00 33 00 65 00 2d 00 34 00 35 00 30 00 65 00 2d 00 39 00 32 00 31 00 32 00 2d 00 37 00 32 00 39 00 31 00 30 00 61 00 39 00 65 00 66 00 38 00 38 00 34 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>6a548083-4b3e-450e-9212-72910a9ef884</Guid>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6666	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6670	2	09 00		success or wait	2	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6674	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 32 00 39 00 3a 00 35 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-23T05:29:51Z</CreationTime>	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6772	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6776	2	09 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6778	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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6818	4	0d 00 0a 00		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD17C.tmp.WERInternalMetadata.xml	6822	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	7FF8BB60E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD882.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_188de68a\Report.wer	0	2	fd fd		success or wait	1	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_188de68a\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	7FF8BB60E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_W3X_4b2923b72b8cb92cc1b5f136816e1b8388c8c88_11952a33_188de68a\Report.wer	9590	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 31 00 33 00 36 00 38 00 38 00 36 00 39 00 37 00 33 00	MetadataHash=-136886973	success or wait	1	7FF8BB60E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{50e1f40b-35d9-9514-3dd2-1a291dd85141}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF8BB631D2D	unknown
\REGISTRY\A\{50e1f40b-35d9-9514-3dd2-1a291dd85141}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF8BB631D2D	unknown
\REGISTRY\A\{50e1f40b-35d9-9514-3dd2-1a291dd85141}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FF8BB60E3FE	unknown

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

Analysis Process: svchost.exe PID: **1388**, Parent PID: **604**

General

Target ID:	16
Start time:	22:30:11
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:	0x7ff7e8070000
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: **5268**, Parent PID: **604**

General

Target ID:	18
Start time:	22:30:35
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:	0x7ff7e8070000
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: **4028**, Parent PID: **604**

General

Target ID:	25
Start time:	22:31:06
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:	0x7ff7e8070000
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: **5832**, Parent PID: **604**

General

Target ID:	26
Start time:	22:31:10
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:	0x7ff7e8070000
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: **3264**, Parent PID: **604**

General

Target ID:	27
Start time:	22:31:34
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:	0x7ff7e8070000
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: **5528**, Parent PID: **604**

General

Target ID:	29
Start time:	22:31:50
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:	0x7ff7e8070000

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly