ID: 631910
Sample Name: nZNmWqwnpr
Cookbook: default.jbs
Time: 22:35:23
Date: 22/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

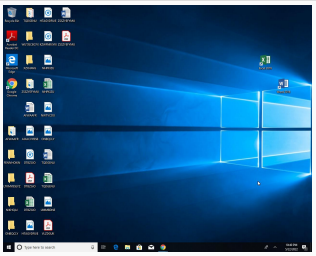
Windows Analysis Report

nZNmWqwnpr

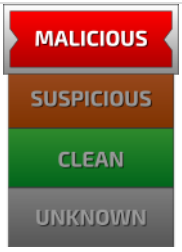
Overview

General Information

Sample Name:	nZNmWqwnpr (renamed file extension from none to dll)
Analysis ID:	631910
MD5:	828a9b1007dc45..
SHA1:	8214993bb314d0.
SHA256:	b59f16ee5e5248..
Tags:	exe trojan
Infos:	



Detection



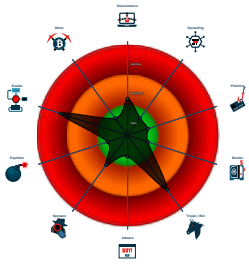
Emotet

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7048 cmdline: loaddll64.exe "C:\Users\user\Desktop\nZNmWqwnpr.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7056 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\nZNmWqwnpr.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7080 cmdline: rundll32.exe "C:\Users\user\Desktop\nZNmWqwnpr.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 3368 cmdline: C:\Windows\system32\WerFault.exe -u -p 7080 -s 336 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - regsvr32.exe (PID: 7068 cmdline: regsvr32.exe /s C:\Users\user\Desktop\nZNmWqwnpr.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6208 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\PDQmdReNwGSs\ZxyxzMoIe.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 7088 cmdline: rundll32.exe C:\Users\user\Desktop\nZNmWqwnpr.dll,AddIn_FileTime MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 1816 cmdline: C:\Windows\system32\WerFault.exe -u -p 7088 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 7152 cmdline: rundll32.exe C:\Users\user\Desktop\nZNmWqwnpr.dll,AddIn_SystemTime MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4548 cmdline: rundll32.exe C:\Users\user\Desktop\nZNmWqwnpr.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 3348 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6560 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3008 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5808 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5188 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5940 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
00000004.00000000.452085701.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.452594179.000001E59C5C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.449463120.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.449875064.000001E59C5C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.959360306.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.b70000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1e59c5c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.12d0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.b70000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.13e99710000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

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

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

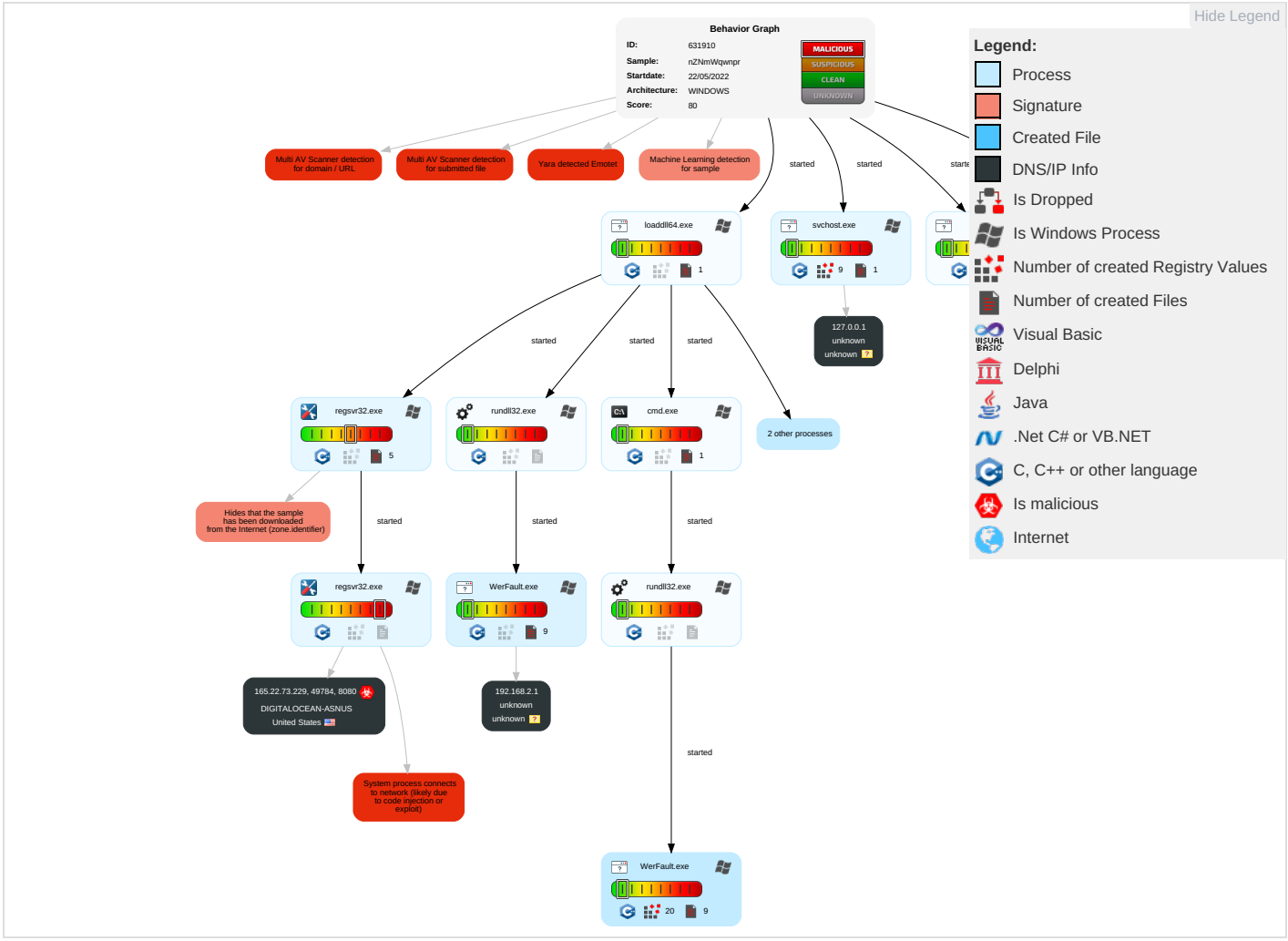
Stealing of Sensitive Information

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 DLL Side-Loading	1 1 1 Process Injection	2 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	3 Virtualization/Sandbox Evasion	LSASS Memory	1 Query Registry	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	4 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	3 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	2 5 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

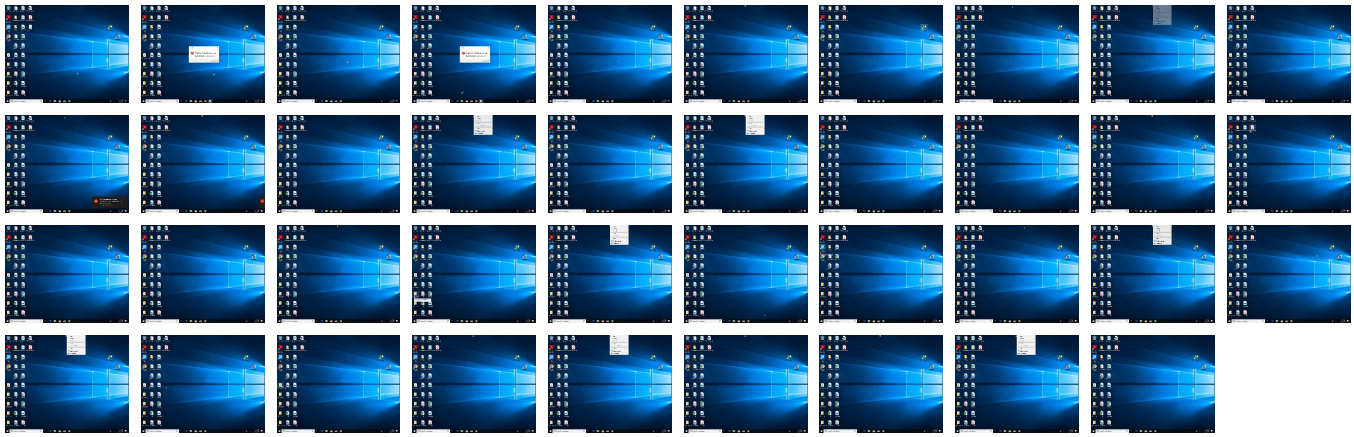
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
nZNmWqwnpr.dll	49%	Virustotal		Browse
nZNmWqwnpr.dll	59%	ReversingLabs	Win64.Trojan.Emotet	
nZNmWqwnpr.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.b70000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.13e99710000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.13e99710000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.13e99710000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.1e59c5c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
4.0.rundll32.exe.1e59c5c0000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
8.2.regsvr32.exe.12d0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.0.rundll32.exe.1e59c5c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://165.22.73.229/	7%	Virustotal		Browse
http://https://165.22.73.229/	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/tem	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/	2%	Virustotal		Browse
http://https://165.22.73.229:8080/	0%	Avira URL Cloud	safe	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

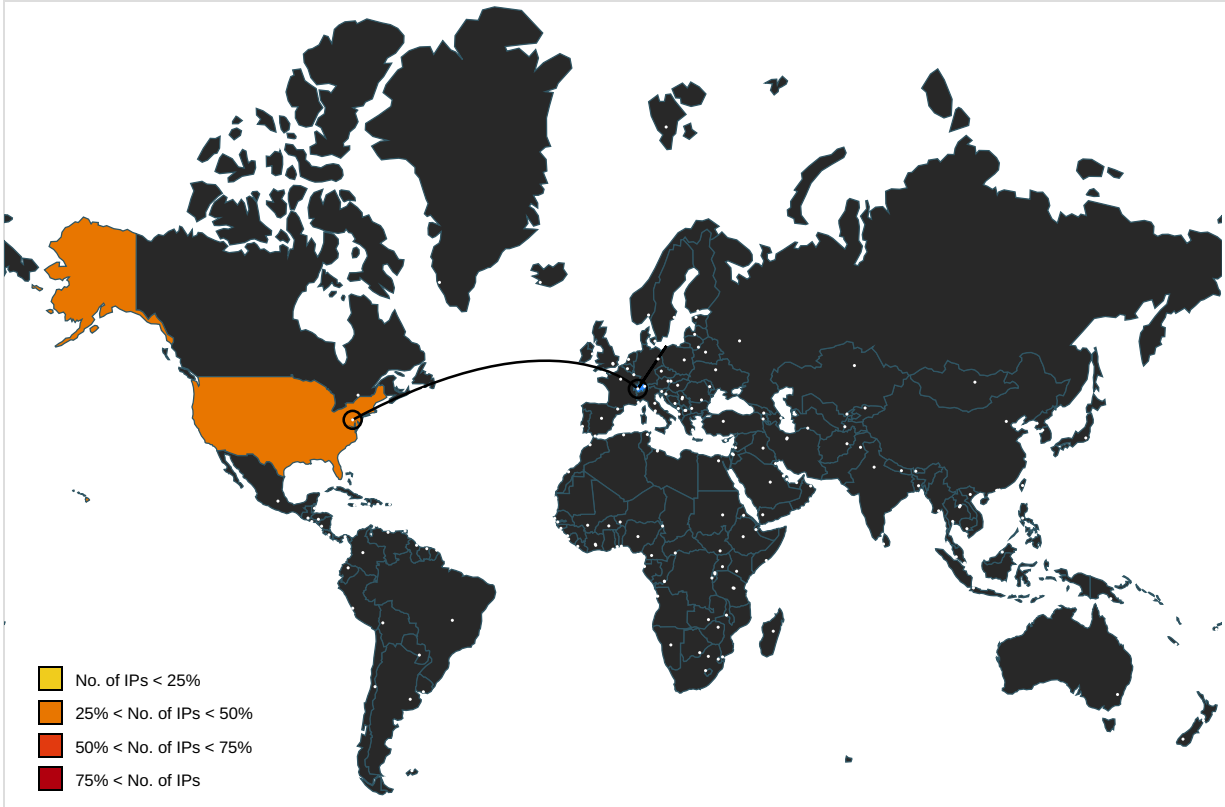
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://165.22.73.229/	regsvr32.exe, 00000008.00000002.95903544 1.0000000001341000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 008.00000003.521676384.0000000001341000. 00000004.00000020.00020000.00000000.sdmp	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001B.00000003.737868944 .000002075EB94000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ver)	svchost.exe, 0000000D.00000002.842956672 .0000024A18088000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000002.762109790.000002075E0EA000.00 000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001B.00000003.737868944 .000002075EB94000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001B.00000003.741783275 .000002075F002000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 B.00000003.741717338.000002075EB94000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://165.22.73.229:8080/tem	regsvr32.exe, 00000008.00000002.95903544 1.0000000001341000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 008.00000003.521676384.0000000001341000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://help.disneyplus.com.	svchost.exe, 0000001B.00000003.737868944 .000002075EB94000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 0000001B.00000003.732764832.000002075F002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.732695709.000002075EB94000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.732742125.000002075EBA5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229:8080/	regsvr32.exe, 00000008.00000002.959035441.0000000001341000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000003.521676384.0000000001341000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000008.00000002.958979074.0000000001308000.00000004.00000020.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001B.00000003.732764832.000002075F002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.732695709.000002075EB94000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.732742125.000002075EBA5000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000001B.00000003.732764832.000002075F002000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.732695709.000002075EB94000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001B.00000003.732742125.000002075EBA5000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001B.00000003.737868944.000002075EB94000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

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:	631910
Start date and time: 22/05/202222:35:23	2022-05-22 22:35:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nZNmWqwnpr (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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.evad.winDLL@23/13@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 73% (good quality ratio 38.9%) • Quality average: 32.7% • Quality standard deviation: 37.6%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.21, 13.89.179.12, 23.54.113.104, 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, onedsblobprdcus17.centralus.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:36:55	API Interceptor	2x Sleep call for process: WerFault.exe modified

Time	Type	Description
22:37:07	API Interceptor	11x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

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

Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.2494459593111375
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU42:BJiRdwfu2SRU42
MD5:	350E7E51EE85D4C9CE2C637486617909

SHA1:	37BD386501593C088CD673DA09E861BABDA8CDCC
SHA-256:	682ED1F34B514551258D72C152ED274023F97A9CD5CAF46555653C72F49A82F8
SHA-512:	E9907CC6902875ABCED0F51A2391C5510FD4AB5884E019EB8939E4CEAC21DD9EEFC3E901D57C4E06AC24B08D32C38113A97893C20BC59BDC2737F2AF83592618
Malicious:	false
Preview:	V.d.....@..@.3...w.....3...w.....C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....d#.....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x0770f373, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25068119477366796
Encrypted:	false
SSDEEP:	384:C3X+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:C3cSB2nSB2RSjlK/+mLesOj1J2
MD5:	1480EA214CAB080BEDFC3ED714D746F4
SHA1:	0EAC25CDC2831C465EA5A04F8871AC0F9C63558B
SHA-256:	F4E05B52FE784CA576AC6E31DEBE983DC39034BEE1C2A49CA617D658ADE14BF8
SHA-512:	9356982BE6ECAC443164963AE37D98427645D6A0425AEB2B84D997AF0B9833596F5DE0086F737E8A6B313850204B7F51D08756DB92E04E0EAEB2F8B09D6A310A
Malicious:	false
Preview:	.p.s... .....e.f.3...w.....).....(...z...%...z..h.(.....(...z....).....3...w.....B.....@.....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07547562542474998
Encrypted:	false
SSDEEP:	3:S6IlllIJ7viAgk3pFlHgKSiBIAzfymltlfAypFlAll3VkttlmlnI:S9tJriAgcRqAzbFRA3
MD5:	8FF33FD4A420FF92477534CB8CE25320
SHA1:	091CE71394F3A44CE7AFC26267BE628A7D183A71
SHA-256:	0D9EE2910436B74DA503A7A4654096CF94B9A549E619D094EA7BE80EE1224C45
SHA-512:	61B35872189BC888F21F4BDAAC68FEC3A8390AA0498410D00387197CB7E4BB61FAF3D485EA4BB7342A1C7FCCA4577A04D193459D76E9203137700E9922AB80BE
Malicious:	false
Preview:	|.|.....3...w...%...z...(...z.....(...z...(...z...y~..(...zWg.....4.O.(...z.....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_074e79e0\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):	0.7854483740623535
Encrypted:	false
SSDEEP:	96:DgFVgGbiDJJPny8ji55o+7Rl6tpXIQcQ5c6ZucE1cw3CzXaXz+HbHgSQgJPbzIDG:s7iNJKwHXkfGDjV9/u7s1S274ltT
MD5:	10A3CCFB064C4C0008134CF070C0AD65
SHA1:	B7584F04137F5C47095AE005A7DBF67C22AD3B8A
SHA-256:	FD7CCAAD2B49D18EE75090C51929C2859B44509E290D02B0AD3A9BC14A76854E
SHA-512:	D892BC67A59176C8246B6ECC9AEE1994092EAAE7AFAFEE608632EAF765D55578852D51AC8E73DD949461200B2639EE02CC946F8630EC33D7A6441DD081CEF5AA

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.=.1.3.2.9.7.7.5.7.8.1.0.1.5.2.8.6.4.1.....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.=.1.3.2.9.7.7.5.7.8.1.2.6.0.5.9.8.4.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.2.e.8.5.5.d.0.-.7.9.7.0.-.4.c.6.d.-.9.0.b.e.-.c.1.f.7.c.b.0.6.5.1.9.9... ..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.=.2.2.5.e.6.a.b.2.-.4.d.b.f.-.4.f.e.7.-.b.a.7.c.-.6.f.e.7.6.b.a.3.8.9.6.e.....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._.n.Z.N.m.W.q.w.n.p.r...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.b.0.-.0.0.0.1.-.0.0.1.7.-.8.d.c. 7.-.7.a.1.4.6.7.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1. 4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_0d7e7db9\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):	0.7843612334473168
Encrypted:	false
SSDEEP:	96:u0FqXbiQJPnyMji55o+7Rl6tpXIQcQ5c6ZucE1cw3CzXaXz+HbHgSQgJPbzIDV9+:naiQJKgHXkfGDjV9/u7s1S274ltT
MD5:	7AED913045EC89E659CE045CEA73813C
SHA1:	5036C5BCD3A4C2899AA7A94A66C5AE04DAA64730
SHA-256:	528A73B71E5D9F169CBE3021F130F01B56832D996B0AD9EE488CD62BA7D21C3E
SHA-512:	9B6557667DCE6FB1C1C4B1831B2896EB7791160264AAEA534398C711EC6F06545A26328573252695267D03FC8F84A3A303568C2653F3243EA3B67B38C996ACC6
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.=.1.3.2.9.7.7.5.7.8.0.9.9.3.0.9.0.3.0.....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.=.1.3.2.9.7.7.5.7.8.1.2.3.8.4.0.3.0.8.....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.=.b.e.6.0.2.3.2.3.-.b.c.f.2.-.4.b.0.8.-.9.0.0.f.-.9.8.5.1.0.8.d.0.8.2.c.6... ..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.=.b.7.9.d.8.3.f.9.-.1.e.7.7.-.4.e.9.f.-.a.a.1.4.-.d.0.0.e.d.c.d.7.8.5.6.b.....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._.n.Z.N.m.W.q.w.n.p.r...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.a.8.-.0.0.0.1.-.0.0.1.7.-.3.a.d. 0.-.3.e.1.4.6.7.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1. 4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 05:36:50 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64892
Entropy (8bit):	2.300064149534914
Encrypted:	false
SSDEEP:	384:e04cSe2YqH2DCd/3tcldYngZ5ksPckn1Cpz2tfjCnXJ6bEUSoC:efMqH2DCx3t+ME8e
MD5:	74C9D643CB3A498FE46D0C057027D69A
SHA1:	55225048E60867841D51769639BE22A1626B9148
SHA-256:	8CCB4ADBCD420845E115B1B477678B8188CEA755053EF87022E43AEA8C89D8D5
SHA-512:	007BC05C750C4D72C5058B757856CDC629C6CEC30CE74A2094C88CB82945111CC4BDE7302C3F04131154215D37526397EC629DBB6BC4975AC2DFC9FAB6AD8 2
Malicious:	false
Preview:	MDMP..... .....r..b.....8.....$...d;.....`.....8.....T.....".....$.....U.....B.....P%... ...Lw.....Q...T.....h..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\WER658D.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon May 23 05:36:51 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	65264
Entropy (8bit):	2.28612973826541
Encrypted:	false
SSDEEP:	192:5VKVLM04cqPyowuCSrMV/qkm+s494F1sOC5qCt073S/wmsg3HXdOYXqf1XItVzwi:704cSe2YqH2ACACtns2cldYnzw9OG
MD5:	4650085A66CEE77078C7A0F4F3FCBC63
SHA1:	05B8304B00050B702A35DD97770DC07DD341F525
SHA-256:	BF99D9FC263C89250AC1FD269D0330F8AC27AC7BD5836367E7CB924A16B73120
SHA-512:	2EB6AB89F891F91C1ABE2E7A96152F62F17212BCC9BB36F14FC8BFF537861F6C85B6D1EFE639E660E5B6B018D90BDCB1A1B714C3C303F319FB27B16D3E4060 5
Malicious:	false

Preview:	MDMP..... .....s..b.....8.....$...d;.....`.....8.....T.....X.....".....$.....U.....B.....P%... ...Lw.....^....T.....i..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\WER6996.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):	8652
Entropy (8bit):	3.696860486924025
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyjIm3aVh6YfDSDgmfDbSXuCprV89bgqHfeAm:RrlsNiEIm3aVh6YrSDgmfDbSEgifg
MD5:	F0A6A498E352C9D3F2357A69DC8EFFFA
SHA1:	C224333CEBE3BC1428C4C05C4A2B70728C42FABD
SHA-256:	60C8E096886E5CDD826E43084D6D00B8DCAA1C2603A0AB36F0CBE1A9696576CA
SHA-512:	9D8D7F2BB2ED11A87D8326980A36C5AD2252D714E0657DE45D5EECC24106135ABF88AD47F4D370DA151F0B4E57BD0817A2AD8BC8C7B6778BEF33FD57CDC8F 1F
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.8. 0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8646
Entropy (8bit):	3.695404074543651
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiajo9IaDX6YCMLgmfDbSXuCprT89bgCHfAAm:RrlsNico9IaDX6YJLgmfDbSCg6f+
MD5:	644F9078CD7E5D0A6E19370A1E1F2531
SHA1:	C90B431C35BBFB97EEB3B1E1EF70E01188345E7D
SHA-256:	149EB0DC890DD50BC591A1750E78454A3EAE36B84BFD30CB51615C12BD1940A6
SHA-512:	E73DB170EEEF31EA430D07A9BC437DAD2B4B85857FF7CCD76854132FE76A4CFE406BC9B04A54F146D9ABEF6693F9459DC82C2FF284A8B4402A064C36AF5056 A2
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.7.0.8. 8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6BC9.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):	4.49728997291251
Encrypted:	false
SSDEEP:	48:cvIwSD8zsOJgtBI98qWgc8sqYjB8fm8M4JCUUCU33nFsVyq8vhU33OZESC5Sad:uITfESLgrsqYqJRiaVW2uVvad
MD5:	928EA0F3D8EAF23625C894019743EFA6
SHA1:	0B203361083F47FA052009E94D2F38C5A1307462
SHA-256:	B3DC63A3F71D2C676D3324E8630505545441B28397045BDE4E54420F1909D507
SHA-512:	439FF7AEEBFC7B2523DCA5334977346CDEF3253B194074C7A413CB21850644924C0A5D3DB4FDF28CD52A3B01192E3BF7FB4A62E503FE8EB006BD953471D19D C
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="1527287" />.. <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\WER6D02.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):	4.498305108452743
Encrypted:	false
SSDEEP:	48:cvIwSD8zsOJgtBI98qWgc8sqYjv8fm8M4JCUUCU33nFDyq8vhU33gutZESC5S4d:uITfESLgrsqY4JRiFW2XVv4d
MD5:	E55C5123469E90644C2DA6D071072E0E
SHA1:	C0419D22B7CDECEF35DCC1D0E58639DBA892287F
SHA-256:	879F151CD90E93887BD195E51B3384D962F3B2A9102EFD45749AC63D68D20135
SHA-512:	21CE0A353B0AF16A64FB6FD7B90836B05FC1A92FFA922C537C8EFCF12C7A3C7204D65C2433E9314BA919C82719EB9171F31B3B05F842EF47B8C70FCE1BE4F703
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="1527287" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp

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

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	7.1527203772082135
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:	nZNmWqwnpr.dll
File size:	371200
MD5:	828a9b1007dc45671d8a58e240c7c973
SHA1:	8214993bb314d0f4c1889e507f88beeb3f6e5b63
SHA256:	b59f16ee5e524814316a8be8ef54ea02f9a496267555e65eeb585e4ade85ffec
SHA512:	7519b39dd811c3578e0002d5c4f35b2a6855092978004ecb2ca0030c1550aa3d38b346f83c43eb286ab9e1bf6209050078286ddb8bfea5f1d5dc3efcaafeeeef
SSDEEP:	6144:hlNuuXQASByX7YxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7Qy/BJ7rGTK/V3
TLSH:	34848E46F7F551E5E8F7C13889A23267F9317C948B38A7CB8A44466A4F70BA0E93D701

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

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

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

Entrypoint Preview

Instruction
dec esp
mov dword ptr [esp+18h], eax
mov dword ptr [esp+10h], edx
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 28h
cmp dword ptr [esp+38h], 01h
jne 00007F9D84D5F587h
call 00007F9D84D648E7h
dec esp
mov eax, dword ptr [esp+40h]
mov edx, dword ptr [esp+38h]
dec eax
mov ecx, dword ptr [esp+30h]
call 00007F9D84D5F594h
dec eax
add esp, 28h
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
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 00007F9D84D5F592h
cmp dword ptr [00028DE8h], 00000000h
jne 00007F9D84D5F589h
xor eax, eax
jmp 00007F9D84D5F6A4h
cmp dword ptr [esp+58h], 01h
je 00007F9D84D5F589h
cmp dword ptr [esp+58h], 02h
jne 00007F9D84D5F5D0h
dec eax
cmp dword ptr [0001ED99h], 00000000h
je 00007F9D84D5F59Ah
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 00007F9D84D5F599h
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call 00007F9D84D5F2EAh
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
jne 00007F9D84D5F589h
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	

Name	Virtual Address	Virtual Size	Is in Section
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	4.41538934251	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2b000	0x3798	0x1400	False	0.161328125	data	2.21550179132	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x2f000	0xfcc	0x1000	False	0.5048828125	data	5.08183440168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x30000	0x2e9fc	0x2ea00	False	0.887011980563	data	7.85049584102	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5f000	0x6fc	0x800	False	0.21435546875	data	2.34217115221	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Exports

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

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

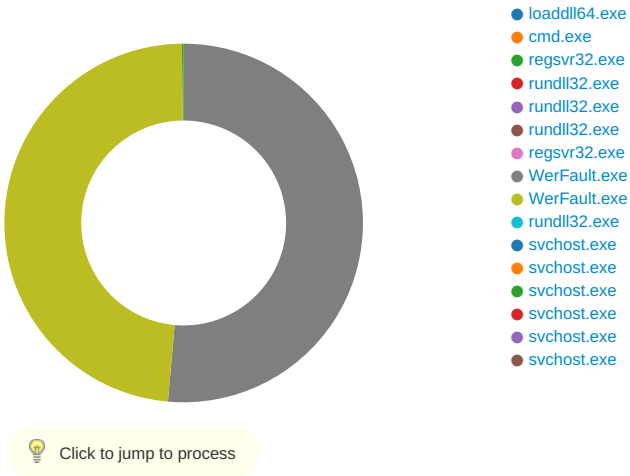
Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 22:37:18.705168009 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:37:18.747581005 CEST	8080	49784	165.22.73.229	192.168.2.5
May 22, 2022 22:37:18.747788906 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:37:19.025082111 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:37:19.067395926 CEST	8080	49784	165.22.73.229	192.168.2.5
May 22, 2022 22:37:19.076613903 CEST	8080	49784	165.22.73.229	192.168.2.5
May 22, 2022 22:37:19.076643944 CEST	8080	49784	165.22.73.229	192.168.2.5
May 22, 2022 22:37:19.076785088 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:37:19.943077087 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:37:19.985933065 CEST	8080	49784	165.22.73.229	192.168.2.5
May 22, 2022 22:37:19.986109018 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:37:20.006026983 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:37:20.092487097 CEST	8080	49784	165.22.73.229	192.168.2.5
May 22, 2022 22:37:20.257360935 CEST	8080	49784	165.22.73.229	192.168.2.5
May 22, 2022 22:37:20.257524014 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:37:23.259675026 CEST	8080	49784	165.22.73.229	192.168.2.5
May 22, 2022 22:37:23.259701967 CEST	8080	49784	165.22.73.229	192.168.2.5
May 22, 2022 22:37:23.259865999 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:39:07.222834110 CEST	49784	8080	192.168.2.5	165.22.73.229
May 22, 2022 22:39:07.222863913 CEST	49784	8080	192.168.2.5	165.22.73.229

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 7048, Parent PID: 2992

General

Target ID:	0
Start time:	22:36:39
Start date:	22/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\nZNmWqwnpr.dll"
Imagebase:	0x7ff710480000
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: 7056, Parent PID: 7048

General

Target ID:	1
Start time:	22:36:40
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\nZNmWqwnpr.dll",#1
Imagebase:	0x7ff602050000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 7068, Parent PID: 7048

General

Target ID:	2
Start time:	22:36:40
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\nZNmWqwnpr.dll
Imagebase:	0x7ff6ddd60000
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: 00000002.00000002.450520095.0000000000B70000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.451105173.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\PDQmdReNwGSs\ZxyxzMole.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: **7080**, Parent PID: **7056**

General

Target ID:	3
Start time:	22:36:41
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\nZNmWqwnpr.dll",#1
Imagebase:	0x7ff6845c0000
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: 00000003.00000000.451694832.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.449470100.0000013E99710000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.476624176.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.451994029.0000013E99710000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.449203482.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.477042089.0000013E99710000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **7088**, Parent PID: **7048**

General

Target ID:	4
Start time:	22:36:41
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\nZNmWqwnpr.dll,AddIn_FileTime
Imagebase:	0x7ff6845c0000
File size:	69632 bytes

MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.452085701.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.452594179.000001E59C5C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.449463120.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.449875064.000001E59C5C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.472954607.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.476424709.000001E59C5C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **7152**, Parent PID: **7048**

General

Target ID:	5
Start time:	22:36:45
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\nZNmWqwnpr.dll,AddIn_SystemTime
Imagebase:	0x7ff6845c0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **6208**, Parent PID: **7068**

General

Target ID:	8
Start time:	22:36:45
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\PDQmdReNwGSs\ZxyxzMoIe.dll"
Imagebase:	0x7ff6ddd60000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.959360306.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.958917594.00000000012D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: **3368**, Parent PID: **7080**

General

Target ID:	9
Start time:	22:36:48
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 7080 -s 336
Imagebase:	0x7ff76a840000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA607F527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6BC9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6BC9.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_0d7e7db9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_0d7e7db9\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6BC9.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6BC9.tmp.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER479D.tmp.csv	success or wait	1	7FFA607EE9F7	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER480B.tmp.txt	success or wait	1	7FFA607EE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 72 1d fd 62 fd 05 12 00 00 00 00 00	MDMP rb	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.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 0f fd 51 02 00 00 54 05 00 00 fd 03 00 00 fd 1b 00 00 68 1d fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBP%LwQThb0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	10276	1232	fd 37 51 fd 3e 01 00 00 7d 45 40 71 fd 7f 00 00 00 00 5c fd fd 7f 00 00 fd 0b 15 fd 3e 01 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 fd fd 1c 43 6e 00 00 00 00 5c fd fd 7f 00 00 00 00 5c fd fd 7f 00 00 00 00 5c fd fd 7f 00 00 18 fd 53 5a 26 00 00 00 fd fd 53 5a 26 00 00 00 1c 00 0f 00 00 00 00 00 fd fd 53 5a 26 00 00 00 16 53 50 fd 3e 01 00 00 0a 00 00 00 00 00 00 00 28 22 65 4a fd 0f 00 00 fd fd fd fd fd fd fd fd fd 52 50 fd 3e 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 15 51 fd 3e 01 00 00 fd 00 00 00 00 00 00	7Q>}E@q\>_3++S++Cn\\ \SZ&SZ&SZ&SP> ("eJRP>hQ>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	1632	168	fd 1b 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	15204	20	52 00 00 00 00 fd 02 fd 01 00 00 00 06 00 00 00 fd 40 00 00	R@	success or wait	82	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	16520	6	01 04 01 00 04 22	"	success or wait	81	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	50132	9416	fd 57 fd 6f fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 78 5a 26 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Wo`xZ&H	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	11508	1232	28 fd 53 5a 26 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 38 fd 53 5a 26 00 00 00 fd fd fd fd fd fd fd fd 38 fd 53 5a 26 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 53 5a 26 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 38 fd 53 5a 26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 82 73 fd 7f 00	(SZ& 3++S++F8SZ&8SZ&SZ& 8SZ&s	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	1900	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 78 5a 26 00 00 00 fd fd 5a 26 00 00 00 48 0b 00 00 fd fd 00 00 fd 04 00 00 fd 36 00 00	xZ&Z&H6	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	9558	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	4556	4344	00 00 23 6e fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 0a 28 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 53 01 00 00 04 00 00 00 fd fd 73 fd 7f 00 00 fd fd 73 fd 7f 00 00 00 00 03 fd 01 00 00 00 fd 27 fd 16 67 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 01 00 00 00 00 00	#n<2|h+(BB?#`A pSss'gnS	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	8908	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 50 fd 02 00 00 00 00 00 60 fd 02 00 00 00 00 4f 0c 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 3b fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 fd 15 1b 00 00 00 00 00 7e fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 00 06 00 00 00 00 00 28 26 61 00 00 00 00 6e 84 1d 00 00 00 00 fd 46 fd 20 00 00 00 00 fd 45 05 01 00 00 00 00 fd 23 01 00 0b fd 00 00 6d fd 05 00 4c fd 0a 00 7e fd 04 00 06 7f 15 00 fd 00 06 00 78 fd 30 00 fd fd 01 00 fd fd 13 00 00 00 00 00 38 52 1e 00 69 60 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 02 00	ZbP`O;~@(&nF E#mL~x08Ri`	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	59548	5344	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 08 00 00 00 46 00 69 00 6c 00 65 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d	EventFileFile(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTim	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER64B3.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 fd 10 00 00 38 12 00 00 05 00 00 00 24 05 00 00 64 3b 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	8$d;`8T"$	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7080</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 34 00 36 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10465</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1230	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404"> 0</Wow64>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1430	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 35 00 30 00 33 00 38 00 30 00 30 00 33 00 32 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203503800320 </PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1536	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 34 00 30 00 38 00 31 00 37 00 31 00 30 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203408171008</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>26292</PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1822	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 35 00 37 00 34 00 30 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7057408</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>106552</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>106352</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2144	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21568</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2278	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 32 00 31 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21216</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 30 00 39 00 31 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>1830912</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 30 00 39 00 31 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>1830912</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2668	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2722	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2752	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2756	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2762	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2802	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2806	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2814	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 35 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7056</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2844	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2848	2	09 00		success or wait	4	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2856	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2916	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	2920	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3018	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3022	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3030	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 39 00 31 00 35 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10915</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3086	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3176	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3240	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3298	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203370262528</PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3408	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203370262528</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3502	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 39 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>791</PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3588	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 39 00 32 00 30 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2920448</PeakWorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3684	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3688	2	09 00		success or wait	5	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3698	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 38 00 30 00 31 00 36 00 36 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2801664</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3792	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>27840</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	3918	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>27664</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4014	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4018	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4028	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>4208</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4164	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>3664</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4284	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 38 00 35 00 39 00 38 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>2985984</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4360	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4364	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4374	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 33 00 33 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3133440</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4480	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 38 00 35 00 39 00 38 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2985984</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4564	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4620	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4670	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4708	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4756	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4802	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX64</EventType>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4858	4	0d 00 0a 00		success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	4862	2	09 00		success or wait	18	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 6e 00 5a 00 4e 00 6d 00 57 00 71 00 77 00 6e 00 70 00 72 00 2e 00 64 00 6c 00 6c 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe_nZNmW qwnpr.dll</Parameter0>	success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	5652	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	5656	2	09 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	5658	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	5698	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	5702	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	5704	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	5742	4	0d 00 0a 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	5746	2	09 00		success or wait	12	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	5750	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6304	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6308	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6310	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6350	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6354	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6356	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6402	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6496	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6500	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 78 00 76 00 6e 00 6e 00 64 00 61 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>xvnnda, Inc.</SystemManufacturer>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6610	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6614	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 78 00 76 00 6e 00 6e 00 64 00 61 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>xvnnda7,1</SystemProductName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6714	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6718	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6722	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6842	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6846	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 33 00 30 00 37 00 32 00 36 00 32 00 38 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>1613072628</OSInstallDate>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6932	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6936	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	6940	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7042	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7046	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7050	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7118	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7122	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7124	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7164	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7168	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7170	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7204	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7208	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7212	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7308	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7312	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7314	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7350	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7354	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7356	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7380	4	0d 00 0a 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7384	2	09 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7388	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7634	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7638	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7640	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7666	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7670	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 33 00 36 00 3a 00 35 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T05:36:51Z">	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7772	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	7776	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.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 39 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 31 00 35 00 36 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 34 00 31 00 35 00 36 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="409" PID="7080" UptimeMS="4156" TimeSinceCreationMS="4156" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8042	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8046	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8052	182	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 35 00 34 00 35 00 31 00 37 00 37 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5451776" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8234	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8238	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8242	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8262	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8266	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8268	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8306	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8310	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8312	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8350	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8354	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8358	98	3c 00 47 00 75 00 69 00 64 00 3e 00 62 00 65 00 36 00 30 00 32 00 33 00 32 00 33 00 2d 00 62 00 63 00 66 00 32 00 2d 00 34 00 62 00 30 00 38 00 2d 00 39 00 30 00 30 00 66 00 2d 00 39 00 38 00 35 00 31 00 30 00 38 00 64 00 30 00 38 00 32 00 63 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>be602323-bcf2-4b08-900f-985108d082c6</Guid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8456	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8460	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8464	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 33 00 36 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>2022-05-23T05:36:51Z</CreationTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8562	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8566	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8568	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8608	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6996.tmp.WERInternalMetadata.xml	8612	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6BC9.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_0d7e7db9\Report.wer	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_0d7e7db9\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	152	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_0d7e7db9\Report.wer	9584	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 37 00 35 00 34 00 37 00 39 00 39 00 33 00 37 00 33 00	MetadataHash=-754799373	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: WerFault.exe PID: **1816**, Parent PID: **7088**

General

Target ID:	10
Start time:	22:36:48
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 7088 -s 328
Imagebase:	0x7ff76a840000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFA607F527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D02.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D02.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_074e79e0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_074e79e0\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFA607EE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D02.tmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D02.tmp.xml	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER48B8.tmp.csv	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER48E8.tmp.txt	success or wait	1	7FFA607EE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 73 1d fd 62 fd 05 12 00 00 00 00 00	MDMP sb	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.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 5e fd 01 00 00 54 05 00 00 fd 03 00 00 fd 1b 00 00 69 1d 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%Lw^Tib0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	10276	1232	20 45 4b fd fd 01 00 00 7d 45 40 71 fd 7f 00 00 00 00 5c fd fd 7f 00 00 fd 0b fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 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 45 67 6d fd 6e 00 00 00 00 5c fd fd 7f 00 00 00 00 5c fd fd 7f 00 00 00 00 5c fd fd 7f 00 00 fd fd fd fd 00 00 00 10 fd fd fd fd 00 00 00 fd 03 01 00 00 00 00 00 68 fd fd fd fd 00 00 00 6a 5b 4a fd fd 01 00 00 0a 00 00 00 00 00 00 00 28 22 65 4a fd 0f 00 00 fd fd fd fd fd fd fd 00 5b 4a fd fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 10 4b fd fd 01 00 00 fd 00 00 00 00 00 00	EK}E@q_3++S++Egmn \\\hj[J("eJ[JK	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	1632	168	fd 1b 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	15204	20	52 00 00 00 fd 2d 4a fd fd 01 00 00 08 00 00 00 fd 40 00 00	R-J@	success or wait	82	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	16520	8	70 fd fd fd fd 00 00 00	p	success or wait	81	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	59772	256	fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 fd 01 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 fd 01 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 fd 01 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 fd 01 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 fd 01 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd 0f 1f fd 00 00 00 00 00 4c fd 78 fd 01 00 00 fd 04 25 08 03 fd 7f 01 75 03 0f 05 fd fd 2e fd fd fd fd fd fd fd fd fd fd fd fd fd 66 66 0f 1f fd 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 66 66 0f 1f fd 00 00 00 00 00 fd fd fd	.L%u.L%u.L%u.L%u.L%u.L%u.ffff	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	11508	1232	fd eb fd 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd c7 fd fd 00 00 00 fd fd fd fd fd fd fd fd c7 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 28 87 fd fd 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd c7 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 82 73 fd 7f 00	3++S++F(s	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	1900	48	fd 1b 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 7b fd fd 00 00 00 28 fd fd fd fd 00 00 00 fd 08 00 00 fd 77 00 00 fd 04 00 00 fd 36 00 00	{(w6	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	9558	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	4556	4344	00 00 23 6e fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 0a 28 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 53 01 00 00 04 00 00 00 fd fd 73 fd 7f 00 00 fd fd 73 fd 7f 00 00 00 00 03 fd 01 00 00 00 fd 7c 04 17 67 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 01 00 00 00 00 00	#n<2|h+(BB?#`A pSss|gnS	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.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 10 fd 02 00 00 00 00 00 60 fd 02 00 00 00 00 5d 0c 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 40 fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 21 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 00 06 00 00 00 00 00 28 26 61 00 00 00 00 fd fd fd 1d 00 00 00 00 fd 49 fd 20 00 00 00 00 fd 5f 05 01 00 00 00 00 fd 23 01 00 fd fd 00 00 1d fd 05 00 31 fd 0a 00 fd fd 04 00 06 7f 15 00 fd 00 06 00 19 15 31 00 fd fd 01 00 fd fd 13 00 00 00 00 00 3f 75 1e 00 7e 60 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 02 00	Zb`]@[!@(&I _#11?u~`	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.tmp.dmp	60028	5236	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER658D.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7088</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 32 00 39 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10294</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1230	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1316	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1376	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 38 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 03808512 </PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1536	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 34 00 30 00 38 00 31 00 37 00 31 00 30 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>220340817 1008</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 38 00 39 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>26289 </PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 31 00 30 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>70410 24</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>106552</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>106352</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2144	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21600</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2278	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 32 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21248</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 30 00 39 00 31 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>1830912</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 30 00 39 00 31 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>1830912</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2668	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2722	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2752	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2756	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2762	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2802	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2806	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2814	30	3c 00 50 00 69 00 64 00 3e 00 37 00 30 00 34 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>7048</Pid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2844	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2848	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2856	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 36 00 34 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll64.exe</ImageName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2928	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2932	2	09 00		success or wait	4	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	2940	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3030	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3034	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3042	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 31 00 37 00 31 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>11710</Uptime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3086	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3090	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3098	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3176	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3180	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3188	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3240	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3244	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3252	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3296	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3300	2	09 00		success or wait	5	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3310	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 34 00 35 00 31 00 31 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4345114624</PeakVirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3400	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3404	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3414	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 34 00 31 00 31 00 34 00 39 00 36 00 39 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4341149696</VirtualSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 36 00 34 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>641</PageFaultCount>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 33 00 31 00 34 00 32 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2314240</PeakWorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3684	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3688	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 33 00 30 00 36 00 30 00 34 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2306048</WorkingSetSize>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 38 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>28208</QuotaPeakPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	3918	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>20448</QuotaPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4014	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4018	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>4072</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.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 32 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>2984</QuotaNonPagedPoolUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4284	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 35 00 31 00 33 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>475136</PagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4372	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 39 00 32 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>479232</PeakPagefileUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4476	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 35 00 31 00 33 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>475136</PrivateUsage>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4546	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4550	2	09 00		success or wait	4	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4558	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4604	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4608	2	09 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4614	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4664	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4696	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4700	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4702	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4744	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4748	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4750	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4788	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4792	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4796	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX64</EventType>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4852	4	0d 00 0a 00		success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4856	2	09 00		success or wait	18	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	4860	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 6e 00 5a 00 4e 00 6d 00 57 00 71 00 77 00 6e 00 70 00 72 00 2e 00 64 00 6c 00 6c 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe_nZNmWqwnpr.dll</Parameter0>	success or wait	9	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	5646	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	5650	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	5652	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	5692	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	5696	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	5698	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	5736	4	0d 00 0a 00		success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	5740	2	09 00		success or wait	12	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	5744	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6298	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6302	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6304	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6344	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6348	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6350	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6388	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6392	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6396	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6490	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6494	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6498	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 78 00 76 00 6e 00 6e 00 64 00 61 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>xvnnda, Inc.</SystemManufacturer>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6604	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6608	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6612	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 78 00 76 00 6e 00 6e 00 64 00 61 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>xvnnda7,1</SystemProductName>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6708	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6712	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6716	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6840	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6844	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 33 00 30 00 37 00 32 00 36 00 32 00 38 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>1613072628</OSInstallDate>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6926	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6930	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	6934	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7044	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7112	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7116	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7118	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7158	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7162	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7164	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7198	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7202	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7206	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7302	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7306	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7308	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7344	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7348	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7350	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7374	4	0d 00 0a 00		success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7378	2	09 00		success or wait	6	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7382	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7628	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7632	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7634	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7660	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7664	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7666	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 33 00 36 00 3a 00 35 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-23T05:36:51Z">	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7766	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7770	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	7774	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 31 00 30 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 37 00 30 00 38 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 34 00 33 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 33 00 31 00 32 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="410" PID="7088" UptimeMS="4312" TimeSinceCreationMS="4312" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8036	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8040	2	09 00		success or wait	3	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8046	182	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 35 00 34 00 35 00 31 00 37 00 37 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5451776" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8228	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8232	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8236	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8260	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8262	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8300	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8304	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8306	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8344	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8348	2	09 00		success or wait	2	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8352	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 32 00 65 00 38 00 35 00 35 00 64 00 30 00 2d 00 37 00 39 00 37 00 30 00 2d 00 34 00 63 00 36 00 64 00 2d 00 39 00 30 00 62 00 65 00 2d 00 63 00 31 00 66 00 37 00 63 00 62 00 30 00 36 00 35 00 31 00 39 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>02e855d0-7970-4c6d-90be-c1f7cb065199</Guid>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8450	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8454	2	09 00		success or wait	2	7FFA607EE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8458	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 33 00 54 00 30 00 35 00 3a 00 33 00 36 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>2022-05-23T05:36:51Z</CreationTime>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8556	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8560	2	09 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8562	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8602	4	0d 00 0a 00		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6A70.tmp.WERInternalMetadata.xml	8606	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6D02.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_074e79e0\Report.wer	0	2	fd fd		success or wait	1	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_074e79e0\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	152	7FFA607EE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_nZN_5c40899ed0f0541acc9ab16798f8d17fcf421773_56ac50ec_074e79e0\Report.wer	9584	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 31 00 32 00 32 00 31 00 31 00 32 00 33 00 30 00 37 00 30 00	MetadataHash=1221123070	success or wait	1	7FFA607EE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{c4271e08-0b55-73c3-e3ee-c7f66c5eabf6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{c4271e08-0b55-73c3-e3ee-c7f66c5eabf6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA60811D2D	unknown
\REGISTRY\A\{c4271e08-0b55-73c3-e3ee-c7f66c5eabf6}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFA607EE3FE	unknown

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

Analysis Process: rundll32.exe PID: **4548**, Parent PID: **7048**

General

Target ID:	11
Start time:	22:36:49
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\nZNmWqwnpr.dll,DllRegisterServer
Imagebase:	0x7ff6845c0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **3348**, Parent PID: **580**

General

Target ID:	13
Start time:	22:37:06
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:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6560**, Parent PID: **580**

General

Target ID:	16
Start time:	22:37:19
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

General

Target ID:	17
Start time:	22:37:28
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5808**, Parent PID: **580**

General

Target ID:	24
Start time:	22:38:06
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5188, Parent PID: 580

General

Target ID:	25
Start time:	22:38:29
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5940, Parent PID: 580

General

Target ID:	27
Start time:	22:38:45
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff78ca80000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly