ID: 631909
Sample Name: qJhkILqiEA
Cookbook: default.jbs
Time: 22:35:11
Date: 22/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

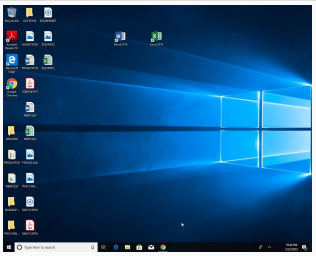
Windows Analysis Report

qJhkILqiEA

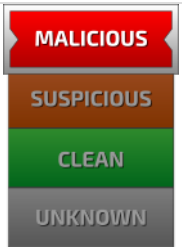
Overview

General Information

Sample Name:	qJhkILqiEA (renamed file extension from none to dll)
Analysis ID:	631909
MD5:	8516983eedc869..
SHA1:	bdd250044234e5.
SHA256:	90498f1ee590da..
Tags:	exe trojan
Infos:	



Detection



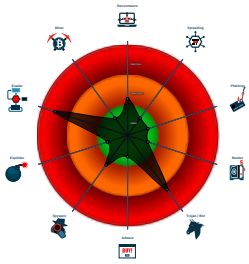
Emotet

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Changes security center settings (n…
- 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…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6012 cmdline: loaddll64.exe "C:\Users\user\Desktop\qJhkILqiEA.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 5772 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\qJhkILqiEA.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 2960 cmdline: rundll32.exe "C:\Users\user\Desktop\qJhkILqiEA.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 6528 cmdline: C:\Windows\system32\WerFault.exe -u -p 2960 -s 352 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - regsvr32.exe (PID: 2320 cmdline: regsvr32.exe /s C:\Users\user\Desktop\qJhkILqiEA.dll MD5: D78B75FC68247E8A63ACBA846182740E)
      - regsvr32.exe (PID: 6448 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JTkGafd\eTKTE.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
    - rundll32.exe (PID: 6236 cmdline: rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,AddIn_FileTime MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 6544 cmdline: C:\Windows\system32\WerFault.exe -u -p 6236 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - rundll32.exe (PID: 6412 cmdline: rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,AddIn_SystemTime MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 6552 cmdline: rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 6616 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6772 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6848 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6912 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6952 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6972 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 3024 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 7004 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5164 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2944 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6476 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5884 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6364 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.276299390.00000000010B0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.275085692.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.273091773.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.301040705.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000000.275341515.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.regsvr32.exe.2430000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.14b00000000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.0.rundll32.exe.1bb54e00000.2.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.10b0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.14b00000000.0.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

Antivirus detection for URL or domain

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)

Lowering of HIPS / PFW / Operating System Security Settings

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information

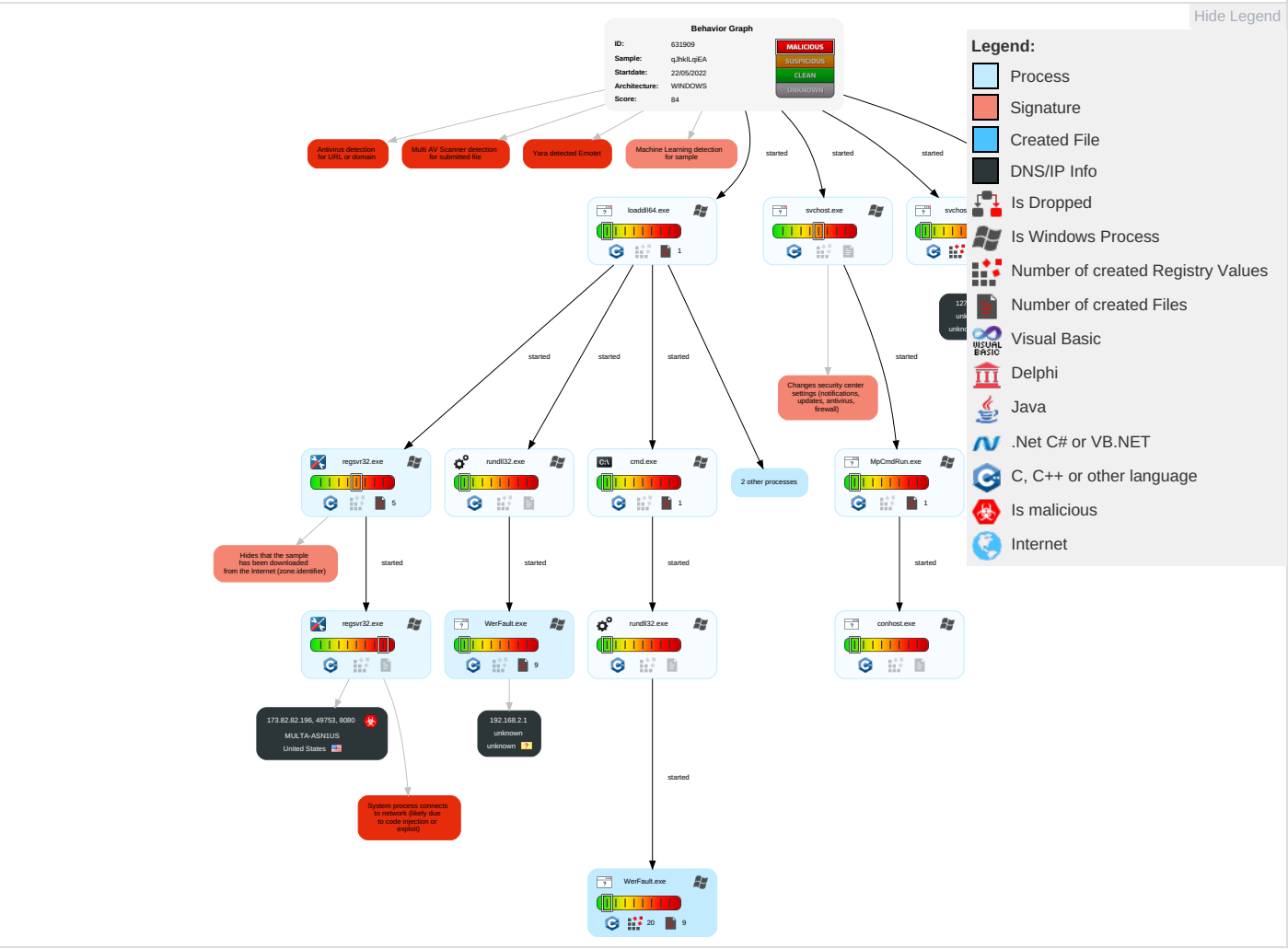
Yara detected Emotet

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	1 Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 1 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	2 Native API	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Virtualization/Sandbox Evasion	Security Account Manager	6 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	3 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Regsvr32	Proc Filesystem	2 5 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Rundll32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 DLL Side-Loading	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 File Deletion	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
qJhkILqiEA.dll	39%	Virustotal		Browse
qJhkILqiEA.dll	59%	ReversingLabs	Win64.Trojan.Emotet	
qJhkILqiEA.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://173.82.82.196:8080/tem	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://www.tiktok.com/legal/report	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/4	100%	Avira URL Cloud	malware	
http://https://173.82.82.196/	100%	URL Reputation	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/	100%	URL Reputation	malware	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/X	100%	Avira URL Cloud	malware	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

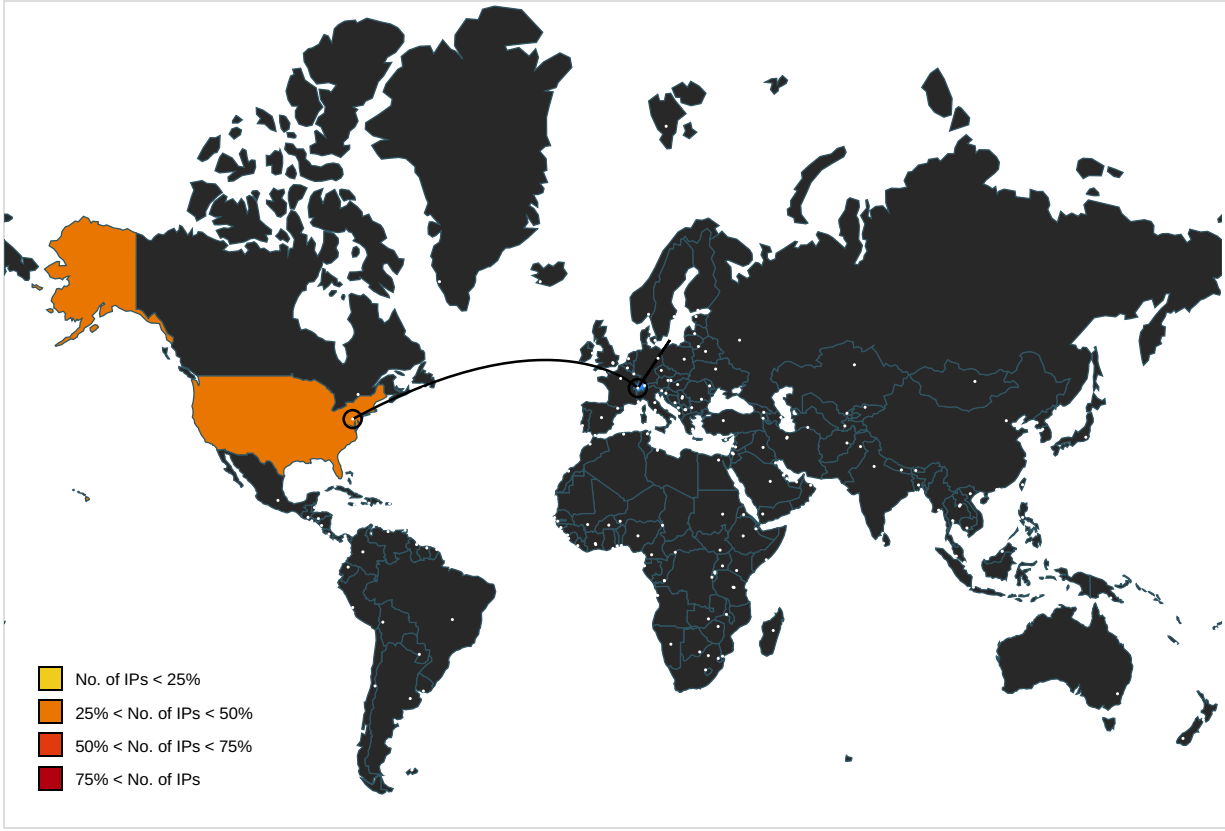
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000010.00000002.326446385.000001EEBD43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000010.00000003.325811178.000001EEBD461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000010.00000002.326446385.000001EEBD43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000010.00000002.326477827.000001EEBD456000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325925433.000001EEBD450000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325821699.000001EEBD44D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000010.00000003.325811178.000001EEBD461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000010.00000002.326457641.000001EEBD442000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325856156.000001EEBD440000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325882596.000001EEBD441000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000010.00000003.325811178.000001EEBD461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000010.00000003.325834208.000001EEBD449000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000010.00000003.303858019.000001EEBD430000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://173.82.82.196:8080/tem	regsvr32.exe, 00000009.00000002.77951843 5.0000000000BA2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 009.00000003.573842211.0000000000BA2000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http:// https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000010.00000002.326457641 .000001EEBD442000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 0.00000003.325856156.000001EEBD440000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325882596 .000001EEBD441000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000026.00000003.616553473 .00000245077AA000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 6.00000003.616691918.0000024507787000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.616612672 .00000245077B4000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 6.00000003.616639931.0000024507C02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.616586218 .0000024507798000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 6.00000003.616569796.0000024507787000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000026.00000003.616553473 .00000245077AA000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 6.00000003.616691918.0000024507787000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.616612672 .00000245077B4000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 6.00000003.616639931.0000024507C02000.00 000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.616586218 .0000024507798000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000002 6.00000003.616569796.0000024507787000.00 000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.tiktok.com/legal/report	svchost.exe, 00000026.00000003.624893055 .0000024507789000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.bingmapsportal.com	svchost.exe, 00000010.00000002.326155574 .000001EEBD413000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000010.00000003.303858019 .000001EEBD430000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 0.00000002.326446385.000001EEBD43D000.00 000004.00000020.00020000.00000000.sdmp	false		high
http:// https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000010.00000003.325811178 .000001EEBD461000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000026.00000003.620962483 .00000245077AB000.00000004.00000020.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://173.82.82.196:8080/4	regsvr32.exe, 00000009.00000002.77951843 5.0000000000BA2000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 009.00000003.573842211.0000000000BA2000. 00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000010.00000003.325856156 .000001EEBD440000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 0.00000003.325877149.000001EEBD445000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 00000010.00000002.326502045 .000001EEBD469000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000001 0.00000003.325786484.000001EEBD467000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000010.00000002.326446385 .000001EEBD43D000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http:// https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 00000010.00000003.303858019 .000001EEBD430000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000010.00000003.325856156.000001EEBD440000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325877149.000001EEBD445000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196/	regsvr32.exe, 00000009.00000002.779518435.0000000000BA2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.573842211.0000000000BA2000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://crl.ver)	svchost.exe, 00000015.00000002.667067807.00000233A6413000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000010.00000003.325856156.000001EEBD440000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000002.326463887.000001EEBD44B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325834208.000001EEBD449000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000026.00000003.624813083.00000245077B0000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.624938666.0000024507C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.624922280.000002450779A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.624893055.0000024507789000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.624832618.00000245077B0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000010.00000002.326155574.000001EEBD413000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000002.326446385.000001EEBD43D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 0000000E.00000002.779831348.000001E2D8843000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000010.00000002.326477827.000001EEBD456000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325925433.000001EEBD450000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325821699.000001EEBD44D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000010.00000003.325811178.000001EEBD461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000010.00000003.303858019.000001EEBD430000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000010.00000003.325811178.000001EEBD461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000026.00000003.616553473.00000245077AA000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.616691918.0000024507787000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.616612672.00000245077B4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.616639931.0000024507C02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.616586218.0000024507798000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000026.00000003.616569796.0000024507787000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196:8080/	regsvr32.exe, 00000009.00000002.779518435.0000000000BA2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000009.00000003.573842211.0000000000BA2000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000010.00000002.326463887.000001EEBD44B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325834208.000001EEBD449000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000026.00000003.620962483.00000245077AB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000010.00000003.303858019.000001EEBD430000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196:8080/X	regsvr32.exe, 00000009.00000002.779344665.0000000000B68000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dynamic.t	svchost.exe, 00000010.00000003.325821699.000001EEBD44D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000010.00000003.325811178.000001EEBD461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://disneyplus.com/legal.	svchost.exe, 00000026.00000003.620962483.00000245077AB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000010.00000003.303858019.000001EEBD430000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000002.326347509.000001EEBD439000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000010.00000002.326463887.000001EEBD44B000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000010.00000003.325834208.000001EEBD449000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 0000000E.00000002.779831348.000001E2D8843000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000010.00000003.325811178.000001EEBD461000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 00000026.00000003.620962483.00000245077AB000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 0000000E.00000002.779831348.000001E2D8843000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000010.00000003.325834208.000001EEBD449000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.82.82.196	unknown	United States		35916	MULTA-ASN1US	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	631909
Start date and time: 22/05/202222:35:11	2022-05-22 22:35:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qJhkILqiEA (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:	40
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:	mal84.troj.evad.winDLL@32/16@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 67.5% (good quality ratio 36%) • 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): 20.189.173.20, 20.42.73.29, 23.54.113.104, 173.222.108.210, 173.222.108.226, 20.223.24.244
- Excluded domains from analysis (whitelisted): a767.dspw65.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, onedsblobprdeus15.eastus.cloudapp.azure.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, onedsblobprdwus15.westus.cloudapp.azure.com, settings-win.data.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.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
22:36:45	API Interceptor	2x Sleep call for process: WerFault.exe modified
22:36:54	API Interceptor	11x Sleep call for process: svchost.exe modified
22:37:50	API Interceptor	1x Sleep call for process: MpCmdRun.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):	0.24947612639605962
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4a:BJiRdwfu2SRU4a
MD5:	20D65F737AC7651971A0AA755D1E7E12
SHA1:	6675199D990A5433EB11EB36FD0AA3559C220DC5
SHA-256:	411B0A8BD735F0620F5DDE39895EFD131D17DCCF5EB25F2296694B910D51E885
SHA-512:	5D12720DD83B469C15800DEC713DA2F2C1CB37F52CA1D6F2C79DFC08C66D7DCC345C49A0F0B267A01F451B9D4A593615D8DA4862174EE00D7E194524415893
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 0xadbf7199, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2505206879766742
Encrypted:	false
SSDEEP:	384:FLu+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:FLBSB2nSB2RSjlK/+mLesOj1J2
MD5:	73394369205269EDEE99F5D26DA68F54
SHA1:	BBC4E6BC8EFCEC7C16D0B4AD815B7861C16EB17C
SHA-256:	58AC059ECE0C37F1E3E4B9DD37EF0E9DB135D4E05C97E89F53FD3BFE07AFBE87
SHA-512:	2CD314095DFE0B026536896D1925BE7E2E33EB5D141606B9AA76A457CEC5F492C40A2303C1CBE9574715C5CA50E1D2F6868570CE1D1B05CF63E6CF2AB467F8 0
Malicious:	false
Preview:	..q.... .....e.f.3...w.....).....(...z..6$...z..h.(.....(...z....).....3...w.....B.....@..... ....'..A.(...z.....4..(...z..... .....

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

Process:	C:\Windows\System32\svchost.exe

File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07358110724839773
Encrypted:	false
SSDEEP:	3:mlT7vTQaslt41gkgNqk9ihNpVWyasltAll3VkttlmlnI:mrO41gpNqT6yNA3
MD5:	D5B239BD9A6FDC26898A229E38204473
SHA1:	9A52385262A2D6272E26291C39D934944E1E0281
SHA-256:	447943F993982FC35D978C0406301AC5263FF255511A6BBF879F90BBE126E9FC
SHA-512:	908413F299141CEC92336CF0BFAD2173C874BB9AA3526980F1F112732960A60BC93C300DBCCFBCB94B04A4563EEF57533BD4EC2698047756E9AEC1670C382DA
Malicious:	false
Preview:	8.!.....3...w..6$...z...(...z.....(...z...(...z..X...(...z.....4..(...z..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19e8067e\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):	0.7859304120709223
Encrypted:	false
SSDEEP:	96:THsiFO01xui4JPnyRjZ55ol7RH6tpXIQcQSc6rcEbcw3dXXaXz+HbHgSQgJPbsIA:T/n1ki4JKPHMvhBjC9/u7sVS274ltY3
MD5:	3CC5050A660AF149D59DD20835EF7835
SHA1:	AC1B7FA95ED16816A2B769E23921A44CF43B5707
SHA-256:	F68FA028840101375487807AE4FAB5A5DBEF84F74A2F120DBC81E67FA65215F4
SHA-512:	D9F3ED055B9753491453CE814E1DEA9066A13F7652CCC302224E57E2886C11108EC921AAD0B0AA6D9856F15E061E92A450A581844A23CA9E4B9FE9F1455F65C
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.=.1.3.2.9.7.7.2.5.3.9.6.2.2.4.0.3.9.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.2.5.4.0.3.8.1.7.7.5.8.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.9.0.4.4.5.c.9.-.e.a.3.6.-.4.6.b.1.-.a.0.f.b.-.8.1.9.6.6.f.e.f.c.6.5.a... ..I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.9.0.8.e.c.4.9.-.0.b.7.2.-.4.5.0.5.-.b.f.c.d.-.7.6.7.2.5.8.b.b.6.b.4.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._.q.J.h.k.I.L.q.i.E.A...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.b.9.0.-.0.0.0.1.-.0.0.1.c.-.4.7.3.3.-.9.c.9.b.1.b.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_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19f80630\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):	0.7865047293153473
Encrypted:	false
SSDEEP:	96:TyTFlRjuiTmJPnyqjZ55ol7RH6tpXIQcQSc6rcEbcw3dXXaXz+HbHgSQgJPbsIDE:TUxyiKJK8HMvhBjC9/u7sVS274ltY3
MD5:	BE8E7AFD6D4D8E250CE1A726779FE8E6
SHA1:	272EE5BBA30B54931D1B9D8A45F5EF07237B37F9
SHA-256:	6EC80542284C3AD85D8F7CD2C0F120E436D3F42F3F5A5FB22261EB906D0556FF
SHA-512:	C83EF3BB0C3CB0F1D4BC056283D8A043D7BCD9B87D8FB8BA4A7720B2C331477053FE131C0D5FB068A98E95A223FA6E472465E37832C02E727B55ED53C3E02ABA
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.=.1.3.2.9.7.7.2.5.3.9.7.2.4.2.4.5.5.1.....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.=.1.3.2.9.7.7.2.5.4.0.4.0.3.9.6.4.9.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.7.a.6.b.d.8.7.-.b.a.b.e.-.4.2.b.b.-.9.b.0.7.-.5.5.f.f.f.6.2.1.9.8.0.7... ..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.=.4.a.c.8.c.9.e.2.-.e.1.1.3.-.4.5.1.5.-.8.e.a.0.-.0.7.2.5.c.8.f.e.3.7.8.8.....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._.q.J.h.k.I.L.q.i.E.A...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.=.0.0.0.0.1.8.5.c.-.0.0.0.1.-.0.0.1.c.-.0.7.8.a.-.1.9.9.c.1.b.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\WERE25C.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun May 22 20:36:37 2022, 0x1205a4 type

Category:	dropped
Size (bytes):	64530
Entropy (8bit):	2.315537384600245
Encrypted:	false
SSDEEP:	384:9kMXiPwsv7fawuClNswEniFpDaCszpNFcp4S:KPPNvz7uClNj6S1gpop4S
MD5:	6E3A6E38BDE0EBAF672E0B152B2E9CF8
SHA1:	15D7C2EAB0A78B5594AE198671074CD3705BC384
SHA-256:	F3EBE8933537C8579E3DDA32ED19A4C49E631206C2C29543A80D4BE47902750F
SHA-512:	4AF1E2B65CA5EA3E91E2FD283C73E6CED6964AADB50C794D8B51E2782EFBDA1E4CB811821313A681F1E493BB13A8EF9A1A3D3F67CD5ADAA15A4DC3A7E55B 7818
Malicious:	false
Preview:	MDMP..... .....b.....8.....p;.....`.....8.....T.....j.....".....$.....U.....B.....\%.....Lw..... .....[.z...T.....b.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERE625.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun May 22 20:36:38 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64134
Entropy (8bit):	2.3132814896368528
Encrypted:	false
SSDEEP:	384:4kMiiPwsv7faw0CsOdswiniF0i0IJlPwwLGn:L0PNvz70CsOdj0S0iV4fn
MD5:	5762DF0D5C2D10CFC58DEC5EDC63512D
SHA1:	102E5BD0BAF25BBF95E64D58355E0542FD2377D4
SHA-256:	C0593FDBF884DFA66D9FE0F5754A5DF0E8FA1B96FA410EFCC0553DB512F14A1F
SHA-512:	53D4EC26D60D6A0201CB240D08D7F75A0DD191F4CE131EEF5E2DB439DE06DA90372F91DBCF43CA2C6154F1B79B92FDDCAA4E9D99D4AF112C9AB930609A3C CD1
Malicious:	false
Preview:	MDMP..... .....b.....8.....p;.....`.....8.....T.....X.....".....$.....U.....B.....\%.... ..Lw.....-.....T.....\.....b.....0.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERE9CF.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8654
Entropy (8bit):	3.7023316502859234
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi4TlURnIWi6YsrggmfWIS6+pr289bplgf0FqDm:RrlsNi8lURnPi6YwggmfWISZpyfeX
MD5:	B8E3028C112C3C71A3CB60C7B7FCDDD0
SHA1:	D38E9FB48CDC23A92AD506C135763E18DF93AB72
SHA-256:	45DC1365195E5C811A19BECCA1668BB85CAAB2B911B04602390C73088BA0ED95
SHA-512:	FD60D614313495F8B70ED5F9A780EC113190C3CC99CF9C8C74C4783CCEAF0DAB24AA72C885DDE1C95C1DB040052D52A80F1B434D7664816E08354BACB6FB7 2B
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.>.2.9.6. 0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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):	8648
Entropy (8bit):	3.7038225115094234

Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiMLLknn7q6YcrEgmfWIS6+pru89bgCjfgAm:RrlsNiQwnn7q6YwEgmfWISBg+fO
MD5:	965DAF269BD9EFCFE40F782FD4698C80
SHA1:	4656D35C5D7E9567670A03FD740745A4FBFD9052
SHA-256:	DB0014AFD19EB60F62AD7842007E2372E17E7E86D26F7EDC87C1C86667BDD6BB
SHA-512:	AEE10F34B4ACA2DC76C8DB1486E51ACFC8197874D5B37946A7338CC583C15AA6450D7907FD1B1C26D648866E21A39B9F03D5C8A43C6C87E4D93A33CEAB249FF
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.2.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD1A.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):	4.512466543323588
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtBI9SkWgc8sqYjD8fm8M4JCGCZgnFCyq8vhZgIZESC5Snd:uITfqQ9grsqYMJ0WHVvnd
MD5:	8F1689406911B2F7E49C47368E43E230
SHA1:	66C4B97D02C8484C78A2E9B59588697D331319C7
SHA-256:	8C292370BB9AA8DAE8FE42A1081425FBB0C06C24AE26CE66875319CFD1557C7C
SHA-512:	E861BE0A7AED138F28FAE5EA383DCA347AC34CA7D2A24923073914613E73F5F49BA69F364115F232B7CECEF952BA81232739F1309C879BF42477801A34B798BA
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="1526747" />.. <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\WERFEFE.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):	4.509638164405873
Encrypted:	false
SSDEEP:	48:cvIwSD8zssJgtBI9SkWgc8sqYjes8fm8M4JCGCZgnFOIyq8vhZgMZESC5S6d:uITfqQ9grsqYiRJgIWDVv6d
MD5:	E9691250CF31B709DDD09DCAB4C634E6
SHA1:	57168296F89C4D8250AE7E143AD264F9AB43432A
SHA-256:	C5298984E457F5D65F87122FCFA189BA9ACADE8CE9162EA40076EF293CC968D5
SHA-512:	F6936C882F01C2D25E3A0D6F11E9BD02A562B7C877173990400C698F7FF5430F724A40D96197DF9C12175DC589B8DAD3E1CE01CC82DCA504C9E79C92060F317
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="1526747" />.. <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:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	330
Entropy (8bit):	3.126909434994818
Encrypted:	false
SSDEEP:	6:kKKHqoJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:SkkPlE99SNxAhUesE1
MD5:	5E35003528F15CD05DB54A3585BB9393
SHA1:	12083A67A69375170A9BD0E64728765AC7536A81
SHA-256:	D7D802C99828C068267463359043F4B4ADDAD7B647084563C88E3B6B07FD3B88
SHA-512:	E252615B1E602E9DE45EB7B2CBEA3BE41181721ADB4EFFCFDE89A5A6C75E3078EC0669A0A5C3A3E47B6D3F3AAD37B261EEB38CFFB09D867AB8F0EFD0E305 212B
Malicious:	false
Preview:	p...... ....E...n..(... ....3k/"[......(...........(...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".8.0.3.3.6.b.2.f.2.2.5.b.d.8.1.:.0."...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA CA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	10844
Entropy (8bit):	3.1613309566460055
Encrypted:	false
SSDEEP:	192:cY+38+DJM+i2Jt+iDQ+yw+f0+rU+0Jtk+EOtF+E7tC+Ewy+9:j+s+i+Z+z+B+c+Y+0g+J+j+u+9
MD5:	1BA198FFF3092A95D17C9CBD2DA7E593
SHA1:	E12CF2DE690D37FF2F70A7ED8C9FB2D270B406AA
SHA-256:	4E911FCFE261EDCEAC5FDC1162387B53C1F96A02216643FB68F8B143612D2C7F
SHA-512:	0AC7019EF4CFB43D56A190A9620445D3A260E29EA77BA3AC63FC40208CE9F215BAFDF45A2FB39E29AE2C70D5B2FCC4B6A65348ED5E96424D43F51ECDF20213 38
Malicious:	false
Preview:	.........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....- .-.............-.

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	7.158106332990621
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:	qJhkILqiEA.dll
File size:	365056
MD5:	8516983eedc8690c1495b828b4262a63
SHA1:	bdd250044234e53e9f08db444a1de00987735930
SHA256:	90498f1ee590da28566434c15efcfd98e829846f233387553ea655fc7559168d
SHA512:	c5b6a37a787a70e70be8614f957c183547b85dfa0913b746f6bc701cec09bd54e04fb53443dfeffedcf83176f581e6a5f4de06219a1fa6d9d015691e9432cd93
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTb0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TWRIvgMSS3AyUrhYu3j
TLSH:	7A747D56F6F110F5E8B7C138C9A23267F8317D559B38A7CB8A08865A4F70BA4E93D740
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...v{.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:	0x62877B76 [Fri May 20 11:28:54 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

Instruction
jne 00007FD4ECB0DDC7h
call 00007FD4ECB13127h
dec esp
mov eax, dword ptr [esp+40h]
mov edx, dword ptr [esp+38h]
dec eax
mov ecx, dword ptr [esp+30h]
call 00007FD4ECB0DDD4h
dec eax
add esp, 28h
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
dec esp
mov dword ptr [esp+18h], eax
mov dword ptr [esp+10h], edx
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 48h
mov dword ptr [esp+20h], 00000001h
cmp dword ptr [esp+58h], 00000000h
jne 00007FD4ECB0DDD2h
cmp dword ptr [00028DE8h], 00000000h
jne 00007FD4ECB0DDC9h
xor eax, eax
jmp 00007FD4ECB0DEE4h
cmp dword ptr [esp+58h], 01h
je 00007FD4ECB0DDC9h
cmp dword ptr [esp+58h], 02h
jne 00007FD4ECB0DE10h
dec eax
cmp dword ptr [0001EDB9h], 00000000h
je 00007FD4ECB0DDDAh
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 [0001EDA3h]
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
je 00007FD4ECB0DDD9h
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call 00007FD4ECB0DB2Ah
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h

Instruction
jne 00007FD4ECB0DDC9h
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	0x2aad0	0x84	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2a204	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x30000	0x2d1fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x2f000	0xfcc	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5e000	0x294	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x22000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x203fa	0x20400	False	0.405969900678	zlib compressed data	5.75556665875	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x22000	0x8b54	0x8c00	False	0.276395089286	data	4.42213983851	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2b000	0x3798	0x1400	False	0.1609375	data	2.22442517754	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x2f000	0xfcc	0x1000	False	0.50537109375	data	5.09571430422	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x30000	0x2d1fc	0x2d200	False	0.922572931094	data	7.88663988983	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5e000	0x6f2	0x800	False	0.21337890625	data	2.33584866509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_FONTDIR	0x300a0	0x2d000	data	English	United States
RT_MANIFEST	0x5d0a0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import

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

Exports

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

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 22:37:03.828249931 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:37:04.001533031 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:04.001677036 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:37:04.024921894 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:37:04.198132038 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:04.216738939 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:04.216763973 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:04.216927052 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:37:08.523586988 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:37:08.696876049 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:08.697592974 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:08.698016882 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:37:08.702534914 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:37:08.891077042 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:09.558660030 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:09.558732986 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:37:12.560230017 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:12.560255051 CEST	8080	49753	173.82.82.196	192.168.2.4
May 22, 2022 22:37:12.560350895 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:38:54.432938099 CEST	49753	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:38:54.432982922 CEST	49753	8080	192.168.2.4	173.82.82.196

Statistics

Behavior

- loaddll64.exe
- cmd.exe
- regsvr32.exe
- rundll32.exe
- rundll32.exe
- rundll32.exe
- regsvr32.exe
- WerFault.exe
- WerFault.exe
- rundll32.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SgrmBroker.exe
- svchost.exe
- svchost.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **6012**, Parent PID: **3700**

General

Target ID:	1
Start time:	22:36:24
Start date:	22/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\qJhkILqiEA.dll"
Imagebase:	0x7ff794690000
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: **5772**, Parent PID: **6012**

General

Target ID:	2
Start time:	22:36:25
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\qJhkILqiEA.dll",#1
Imagebase:	0x7ff7bb450000
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: 2320, Parent PID: 6012

General

Target ID:	3
Start time:	22:36:26
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\qJhkILqiEA.dll
Imagebase:	0x7ff706060000
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: 00000003.00000002.276299390.00000000010B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.276495182.0000000180001000.00000020.00001000.00020000.00000000.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\JTkGafd\eTKTE.dll:Zone.Identifier	success or wait	1	18002AF22	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: 2960, Parent PID: 5772

General

Target ID:	4
Start time:	22:36:26
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\qJhkILqiEA.dll",#1
Imagebase:	0x7ff755bc0000
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: 00000004.00000000.275085692.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.273091773.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.301040705.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.275169745.0000014B00000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.273232804.0000014B00000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.301094896.0000014B00000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6236**, Parent PID: **6012**

General

Target ID:	5
Start time:	22:36:27
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,AddIn_FileTime
Imagebase:	0x7ff755bc0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.275341515.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.300731557.000001BB54E00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.274124592.000001BB54E00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.300443242.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.275509127.000001BB54E00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000000.273887036.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **6412**, Parent PID: **6012**

General

Target ID:	6
Start time:	22:36:31
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,AddIn_SystemTime
Imagebase:	0x7ff755bc0000
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: 6448, Parent PID: 2320

General

Target ID:	9
Start time:	22:36:33
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JTkGafd\eTKTE.dll"
Imagebase:	0x7ff706060000
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: 00000009.00000002.780104900.0000000002430000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.780540136.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: 6528, Parent PID: 2960

General

Target ID:	10
Start time:	22:36:35
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 2960 -s 352
Imagebase:	0x7ff770e00000
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	7FFFEFA3527E	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD1A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD1A.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19e8067e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19e8067e\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD1A.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD1A.tmp.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER18E1.tmp.csv	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1911.tmp.txt	success or wait	1	7FFFEFA2E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 5e fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	9564	6	00 00 00 00 00 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.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 5c 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 5b fd 7a 01 00 00 54 05 00 00 fd 03 00 00 fd 0b 00 00 9e 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 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UB\%Lw[zTb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	10288	1232	fd 38 fd 7a 4b 01 00 00 7d 45 fd 02 fd 7f 00 00 00 00 fd 55 fd 7f 00 00 fd 0b 18 00 4b 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 02 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 7c b0 0b 6e 00 00 00 00 fd 55 fd 7f 00 00 00 00 fd 55 fd 7f 00 00 00 00 fd 55 fd 7f 00 00 18 fd 67 48 13 00 00 00 fd fd 67 48 13 00 00 00 fd 03 01 00 00 00 00 00 fd fd 67 48 13 00 00 00 14 53 fd 7a 4b 01 00 00 0a 00 00 00 00 00 00 00 00 28 42 4e fd fd 0f 00 00 fd fd fd fd fd fd fd fd 52 fd 7a 4b 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 14 fd 7a 4b 01 00 00 fd 00 00 00 00 00 00	8zK}EUK_3++S++|nUUU gHgHgHSzK(BNRzKzK	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	1632	168	30 17 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 30 28 00 00	00(	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	15216	20	5a 00 00 00 00 fd 02 fd 01 00 00 00 2a 00 00 00 14 41 00 00	Z*A	success or wait	90	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	16660	42	01 14 06 00 14 64 0f 00 14 34 0e 00 14 fd 10 70 01 0a 04 00 0a 34 07 00 0a 32 06 70 01 06 02 00 06 72 02 30 01 04 01 00 04 22	d4p42pr0"	success or wait	89	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	59178	8	60 fd 77 48 13 00 00 00	`wH	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	11520	1232	28 fd 67 48 13 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 38 fd 67 48 13 00 00 00 fd fd fd fd fd fd fd 38 fd 67 48 13 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 67 48 13 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 38 fd 67 48 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 02 fd 7f 00	(gH 3++S++F8gH8gHgH8gH	success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	1900	48	fd 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 4b 48 13 00 00 00 28 fd 77 48 13 00 00 00 fd 07 00 00 4a fd 00 00 fd 04 00 00 fd 36 00 00	`KH(wHJ6	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	9570	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	4556	4356	00 00 5d fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 16 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 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 54 01 00 00 00 00 00 00 fd fd fd 02 fd 7f 00 00 fd fd fd 02 fd 7f 00 00 00 fd 02 fd 01 00 00 00 70 fd fd 1b 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 54 01 00 00 00 00 00	]<2|h+(BB?#`A pTpnT	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	8920	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 40 fd 02 00 00 00 00 00 40 17 03 00 00 00 00 2b 56 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 07 fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 58 fd 1a 00 00 00 00 00 fd 44 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 31 04 06 00 00 00 00 00 fd fd 66 3d 00 00 00 00 fd fd fd 1f 00 00 00 00 28 fd fd 22 00 00 00 00 fd fd 0a 01 00 00 00 00 22 3c 01 00 fd 0a 01 00 fd fd 05 00 fd 7c 0a 00 fd 44 05 00 06 7f 15 00 31 04 06 00 fd 5a 34 00 15 fd 01 00 fd fd 14 00 00 00 00 00 24 fd 20 00 fd 56 04 00 4a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 05 00	Zb@@+VXD@1f=("" <|D1Z4$ VJ	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.tmp.dmp	59186	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE25C.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 fd 05 00 00 70 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 6a 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	8p;`8Tj"$	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 32 00 39 00 36 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>2960</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 30 00 39 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12093</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1430	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 35 00 30 00 33 00 38 00 32 00 38 00 39 00 39 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>2203503828992 </PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 35 00 30 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>2203408150528</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1712	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 31 00 33 00 32 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>105013248</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 33 00 36 00 39 00 32 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>7036928</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	1912	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 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 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>106768</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2036	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 35 00 36 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>106568</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2144	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21504</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2278	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 31 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21152</QuotaNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 32 00 32 00 37 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1822720</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2482	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 34 00 36 00 36 00 31 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101466112</PeakPagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 32 00 32 00 37 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1822720</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2752	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2756	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2802	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2806	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2814	30	3c 00 50 00 69 00 64 00 3e 00 35 00 37 00 37 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5772</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2844	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2848	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2916	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2920	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	2928	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3018	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3022	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3030	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 37 00 39 00 34 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12794</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3074	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3078	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3164	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3168	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3228	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3232	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3284	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3288	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 33 00 36 00 39 00 30 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203370369024</PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3394	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3398	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 33 00 36 00 39 00 30 00 32 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203370369024</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3502	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 39 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>794</PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 34 00 30 00 39 00 32 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>2940928</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3684	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3688	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 32 00 32 00 31 00 34 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>28221 44</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	<QuotaPeakPagedPoolU sage>27840 </QuotaPeakPagedPool Usage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage >27664</Qu otaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4014	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4018	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	<QuotaPeakNonPagedP oolUsage>42 08</QuotaPeakNonPage dPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 38 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>3800</QuotaNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 33 00 30 00 30 00 32 00 33 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3002368</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4360	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4364	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4374	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 34 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3149824</PeakPagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4466	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4470	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 33 00 30 00 30 00 32 00 33 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3002368</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4552	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4556	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4610	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4614	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4662	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4666	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4702	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4706	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4750	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4754	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4794	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4798	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4858	4	0d 00 0a 00		success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	4862	2	09 00		success or wait	18	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 71 00 4a 00 68 00 6b 00 49 00 4c 00 71 00 69 00 45 00 41 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_qJhkI LqiEA.dll</Parameter0>	success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	5652	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	5656	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	5698	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	5702	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	5742	4	0d 00 0a 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	5746	2	09 00		success or wait	12	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6304	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6308	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6350	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6354	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6394	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6398	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6496	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6500	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 6e 00 65 00 78 00 68 00 71 00 71 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>nexhqq, Inc.</SystemManufacturer>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6610	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6614	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 6e 00 65 00 78 00 68 00 71 00 71 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>nexhqq7,1</SystemProductName>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6714	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6718	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6842	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6846	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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 39 00 33 00 39 00 33 00 30 00 30 00 35 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>1619393005</OSInstallDate>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6932	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	6936	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7042	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7046	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7050	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7120	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7124	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7126	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7166	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7170	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7172	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7206	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7210	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7214	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7310	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7314	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7316	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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7352	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7356	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7358	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7382	4	0d 00 0a 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7386	2	09 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7390	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7636	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7640	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7642	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7668	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7672	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7674	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 32 00 54 00 32 00 30 00 3a 00 33 00 36 00 3a 00 33 00 38 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-22T20:36:38Z">	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7774	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7778	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	7782	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 35 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 32 00 39 00 36 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 35 00 37 00 33 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 37 00 33 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="415" PID="2960" UptimeMS="5734" TimeSinceCreationMS="5734" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8044	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8048	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8054	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 36 00 36 00 38 00 30 00 35 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="6680576" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8236	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8240	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8244	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8264	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8268	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8270	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8308	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8312	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8314	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8352	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8356	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8360	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 39 00 30 00 34 00 34 00 35 00 63 00 39 00 2d 00 65 00 61 00 33 00 36 00 2d 00 34 00 36 00 62 00 31 00 2d 00 61 00 30 00 66 00 62 00 2d 00 38 00 31 00 39 00 36 00 36 00 66 00 65 00 66 00 63 00 36 00 35 00 61 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>a90445c9-ea36-46b1-a0fb-81966fefc65a</Guid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8458	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8462	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8466	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 32 00 54 00 32 00 30 00 3a 00 33 00 36 00 3a 00 33 00 38 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-22T20:36:38Z</CreationTime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8564	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8568	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8570	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8610	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE9CF.tmp.WERInternalMetadata.xml	8614	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFD1A.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19e8067e\Report.wer	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19e8067e\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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19e8067e\Report.wer	9582	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 35 00 32 00 39 00 39 00 37 00 32 00 39 00 38 00 30 00	MetadataHash=-1529972980	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: WerFault.exe PID: **6544**, Parent PID: **6236**

General

Target ID:	11
Start time:	22:36:35
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 6236 -s 328
Imagebase:	0x7ff770e00000
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	7FFFEFA3527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEFE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEFE.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19f80630	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19f80630\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEFE.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEFE.tmp.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19DD.tmp.csv	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER19FD.tmp.txt	success or wait	1	7FFFEFA2E9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 9e fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	9564	6	00 00 00 00 00 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.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 5c 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 2d fd fd 01 00 00 54 05 00 00 fd 03 00 00 5c 18 00 00 9e 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 fd fd fd 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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 0a 00 00 00 05 00 03 00 00 00 00 00 00 00 00 00 00 00 57 00 2e 00 20 00 45 00 75 00 72 00 6f 00 70 00 65 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	UB\%Lw-T\b0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	10288	1232	fd 03 02 00 00 00 00 00 fd 0b fd 54 fd 01 00 00 00 00 fd 55 fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 fd 7f 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 02 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 21 fd 68 6e 00 00 00 00 fd 55 fd 7f 00 00 00 00 fd 55 fd 7f 00 00 00 00 fd 55 fd 7f 00 00 fd fd 55 08 70 00 00 00 40 fd 55 08 70 00 00 00 fd 03 02 00 00 00 00 00 fd fd 55 08 70 00 00 00 58 5b 47 53 fd 01 00 00 0a 00 00 00 00 00 00 00 28 42 4e fd fd 0f 00 00 fd fd fd fd fd fd fd fd 5a 47 53 fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 10 48 53 fd 01 00 00 fd 00 00 00 00 00 00	TU_3++S++!hnUUUUp@UpUpX[GS(BNZGSHS	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	1632	168	60 18 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 30 28 00 00	`0(	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	15216	20	5a 00 00 00 00 fd 02 fd 01 00 00 00 2a 00 00 00 14 41 00 00	Z*A	success or wait	90	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	16660	42	01 14 06 00 14 64 0f 00 14 34 0e 00 14 fd 10 70 01 0a 04 00 0a 34 07 00 0a 32 06 70 01 06 02 00 06 72 02 30 01 04 01 00 04 22	d4p42pr0"	success or wait	89	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	56058	2840	76 fd fd 02 fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 fd 02 fd 7f 00 00 10 00 00 00 00 00 00 00 28 fd 5d 08 70 00 00 00 21 fd 5d 08 70 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 30 70 08 70 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 41 47 53 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 fd 2f 47 53 fd 01 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	v`2(]p!]p0ppAGS/GSPP	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	11520	1232	00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 55 08 70 00 00 00 fd fd fd fd fd fd fd fd 55 08 70 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 68 fd 55 08 70 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 55 08 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 02 fd 7f 00	3++S++FUpUphUpUp	success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	1900	48	fd 18 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 fd 70 08 70 00 00 00 fd fd fd 08 70 00 00 00 28 04 00 00 fd 4a 00 00 fd 04 00 00 fd 36 00 00	ppp(J6	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	9570	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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	4556	4356	00 00 5d fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 16 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 54 01 00 00 00 00 00 00 fd fd fd 02 fd 7f 00 00 fd fd fd 02 fd 7f 00 00 00 fd 02 fd 01 00 00 00 5b 6e 63 fd 1b 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 54 01 00 00 00 00 00	]<2|h+(BB?#`A pT[ncnT	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	8920	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 30 fd 02 00 00 00 00 00 40 17 03 00 00 00 00 7b 56 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd 03 00 00 00 00 00 fd fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 20 fd 1a 00 00 00 00 00 20 11 05 00 00 00 00 00 40 fd 1f 00 00 00 00 00 31 04 06 00 00 00 00 00 fd fd 66 3d 00 00 00 00 fd 29 10 20 00 00 00 00 fd fc 22 00 00 00 00 fd 1a 0b 01 00 00 00 00 19 3d 01 00 fd 0c 01 00 fd fd 05 00 40 fd 0a 00 20 11 05 00 06 7f 15 00 31 04 06 00 03 0d 35 00 71 fd 01 00 fd 14 00 00 00 00 00 67 3f 21 00 fd 57 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 05 00	Zb0@{V @1f=) "=@ 15qg?!W	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.tmp.dmp	58898	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERE625.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 fd 05 00 00 70 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 2e 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	8p;`8TX."$	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 36 00 32 00 33 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6236</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1178	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 35 00 38 00 37 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12587</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1222	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1226	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1308	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1312	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1368	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1372	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1420	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1424	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 31 00 36 00 37 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 03816704 </PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1526	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1530	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 35 00 30 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>220340815 0528</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1616	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1620	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 38 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>26288 </PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1702	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1706	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1712	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 31 00 37 00 33 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>105017344</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1812	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1816	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 32 00 38 00 37 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7028736</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1902	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1906	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	1912	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 37 00 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 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>106768</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2026	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2030	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2036	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 35 00 36 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>106568</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2134	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2138	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 34 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>21472</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2268	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2272	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2278	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 31 00 32 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21120</QuotaNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2386	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2390	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 31 00 30 00 34 00 33 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>1810432</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2472	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2476	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2578	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2582	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 31 00 30 00 34 00 33 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>1810432</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2660	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2664	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2714	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2718	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2752	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2756	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2802	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2806	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2814	30	3c 00 50 00 69 00 64 00 3e 00 36 00 30 00 31 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6012</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2844	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2848	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2928	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	2932	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3030	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3034	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3042	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 35 00 31 00 34 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>15148</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3086	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3090	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3176	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3180	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3240	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3244	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3296	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3300	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3400	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3404	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3488	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3492	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 30 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>640</PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3574	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3578	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 30 00 31 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2310144</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3684	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3688	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 31 00 39 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2301952</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3778	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3782	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3904	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	3908	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4014	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4018	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4150	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4154	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4270	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4274	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4358	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4362	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4546	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4550	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4604	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4608	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4696	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4700	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4744	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4748	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4788	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4792	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4852	4	0d 00 0a 00		success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	4856	2	09 00		success or wait	18	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 71 00 4a 00 68 00 6b 00 49 00 4c 00 71 00 69 00 45 00 41 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_qJhkILqiEA.dll</Parameter0>	success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	5646	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	5650	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	5692	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	5696	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	5736	4	0d 00 0a 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	5740	2	09 00		success or wait	12	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6298	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6302	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6344	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6348	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6388	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6392	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6490	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6494	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 6e 00 65 00 78 00 68 00 71 00 71 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>nexhqq, Inc.</SystemManufacturer>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6604	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6608	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 6e 00 65 00 78 00 68 00 71 00 71 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>nexhqq7,1</SystemProductName>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6708	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6712	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6840	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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 39 00 33 00 39 00 33 00 30 00 30 00 35 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>1619393005</OSInstallDate>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6926	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	6930	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7040	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7044	70	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 2d 00 30 00 31 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>-01:00</TimeZoneBias>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7114	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7118	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7120	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7160	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7164	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7166	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7200	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7204	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7208	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFI SecureBootEnabled>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7304	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7308	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7310	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7346	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7350	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7352	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7376	4	0d 00 0a 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7380	2	09 00		success or wait	6	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7384	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7630	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7634	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7636	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7662	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7666	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7668	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 32 00 54 00 32 00 30 00 3a 00 33 00 36 00 3a 00 33 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-22T20:36:39Z">	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7768	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7772	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	7776	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 31 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 36 00 32 00 33 00 36 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 35 00 35 00 39 00 33 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 35 00 35 00 39 00 33 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="416" PID="6236" UptimeMS="5593" TimeSinceCreationMS="5593" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8038	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8042	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8048	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 36 00 36 00 38 00 34 00 36 00 37 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="6684672" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8230	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8234	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8238	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8258	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8262	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8264	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8302	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8306	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8308	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8346	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8350	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8354	98	3c 00 47 00 75 00 69 00 64 00 3e 00 33 00 37 00 61 00 36 00 62 00 64 00 38 00 37 00 2d 00 62 00 61 00 62 00 65 00 2d 00 34 00 32 00 62 00 62 00 2d 00 39 00 62 00 30 00 37 00 2d 00 35 00 35 00 66 00 66 00 66 00 36 00 32 00 31 00 39 00 38 00 30 00 37 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>37a6bd87-babe-42bb-9b07-55fff6219807</Guid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8452	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8456	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8460	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 32 00 54 00 32 00 30 00 3a 00 33 00 36 00 3a 00 33 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-22T20:36:39Z</CreationTime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8558	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8562	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8564	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8604	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WEREEF0.tmp.WERInternalMetadata.xml	8608	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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFEFE.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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19f80630\Report.wer	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19f80630\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	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_19f80630\Report.wer	9582	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 33 00 32 00 31 00 35 00 33 00 34 00 35 00 30 00 34 00	MetadataHash=-321534504	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{0b3cecbb-22ab-fd47-0897-64f2253c883d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFFEFA51D2D	unknown
\REGISTRY\A\{0b3cecbb-22ab-fd47-0897-64f2253c883d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFFEFA51D2D	unknown
\REGISTRY\A\{0b3cecbb-22ab-fd47-0897-64f2253c883d}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFFEFA2E3FE	unknown

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

Analysis Process: rundll32.exe PID: **6552**, Parent PID: **6012**

General

Target ID:	12
Start time:	22:36:35
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,DllRegisterServer
Imagebase:	0x7ff755bc0000
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: **6616**, Parent PID: **564**

General

Target ID:	13
Start time:	22:36:39
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:	0x7ff7338d0000
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: **6772**, Parent PID: **564**

General

Target ID:	14
Start time:	22:36:44
Start date:	22/05/2022

Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
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

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6848**, Parent PID: **564**

General

Target ID:	15
Start time:	22:36:46
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

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

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

Analysis Process: svchost.exe PID: **6912**, Parent PID: **564**

General

Target ID:	16
Start time:	22:36:47
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: SgrmBroker.exe PID: **6952**, Parent PID: **564**

General

Target ID:	17
Start time:	22:36:48
Start date:	22/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7e6360000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6972**, Parent PID: **564**

General

Target ID:	18
Start time:	22:36:48
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **7004**, Parent PID: **564**

General

Target ID:	19
Start time:	22:36:49
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff7338d0000
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **5164**, Parent PID: **564**

General

Target ID:	21
Start time:	22:36:53
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:	0x7ff7338d0000
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: MpCmdRun.exe PID: **3024**, Parent PID: **6972**

General

Target ID:	25
Start time:	22:37:49
Start date:	22/05/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff678970000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false

Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	9938	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10120	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 32 00 32 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 32 00 32 00 3a 00 33 00 37 00 3a 00 35 00 30 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sun May 22 2022 22:37:50	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10378	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10464	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF67899BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10484	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10570	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 32 00 32 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 32 00 32 00 3a 00 33 00 37 00 3a 00 35 00 30 00 0d 00 0a 00	MpCmdRun: End Time: Sun May 22 2022 22:37:50	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10670	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF67899BC96	WriteFile

Analysis Process: conhost.exe PID: **5772**, Parent PID: **3024**

General

Target ID:	26
Start time:	22:37:50
Start date:	22/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **2944**, Parent PID: **564**

General

Target ID:	28
Start time:	22:37:59
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7338d0000
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: **6476**, Parent PID: **564**

General

Target ID:	33
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:	0x7ff7338d0000
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: **5884**, Parent PID: **564**

General

Target ID:	35
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:	0x7ff7338d0000
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: **6364**, Parent PID: **564**

General

Target ID:	38
Start time:	22:38:57
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:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Disassembly

No disassembly