ID: 631916
Sample Name: 3vYbe1bYFd
Cookbook: default.jbs
Time: 23:30:10
Date: 22/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

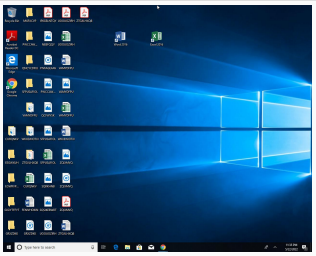
Windows Analysis Report

3vYbe1bYFd

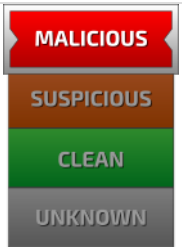
Overview

General Information

Sample Name:	3vYbe1bYFd (renamed file extension from none to dll)
Analysis ID:	631916
MD5:	bf2f633fde70f18…
SHA1:	b3aedb0275ec4f..
SHA256:	663127c151c319..
Tags:	exe
Infos:	



Detection



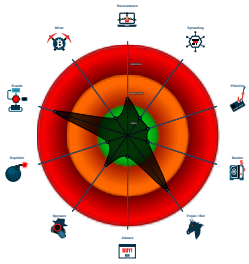
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Multi AV Scanner detection for dom…
- 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: 3196 cmdline: loaddll64.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 5828 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 404 cmdline: rundll32.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 3896 cmdline: C:\Windows\system32\WerFault.exe -u -p 404 -s 336 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - regsvr32.exe (PID: 480 cmdline: regsvr32.exe /s C:\Users\user\Desktop\3vYbe1bYFd.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 4140 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZhCaZiQILulll\dyxOJP.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 4584 cmdline: rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,AddIn_FileTime MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 1404 cmdline: C:\Windows\system32\WerFault.exe -u -p 4584 -s 328 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
  - rundll32.exe (PID: 1260 cmdline: rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,AddIn_SystemTime MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6020 cmdline: rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 6476 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6520 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6560 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6628 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6668 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6732 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6780 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 1348 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 3108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6896 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7052 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6220 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1012 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6292 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
00000007.00000002.761554390.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000002.319251227.0000017C4A5C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000000.245653456.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.246074508.0000017C4A5C0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000004.00000000.245943775.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.rundll32.exe.17c4a5c0000.2.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
2.2.regsvr32.exe.a80000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.a70000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.17c4a5c0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.17c4a5c0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

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

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

Lowering of HIPS / PFW / Operating System Security Settings

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

Stealing of Sensitive Information

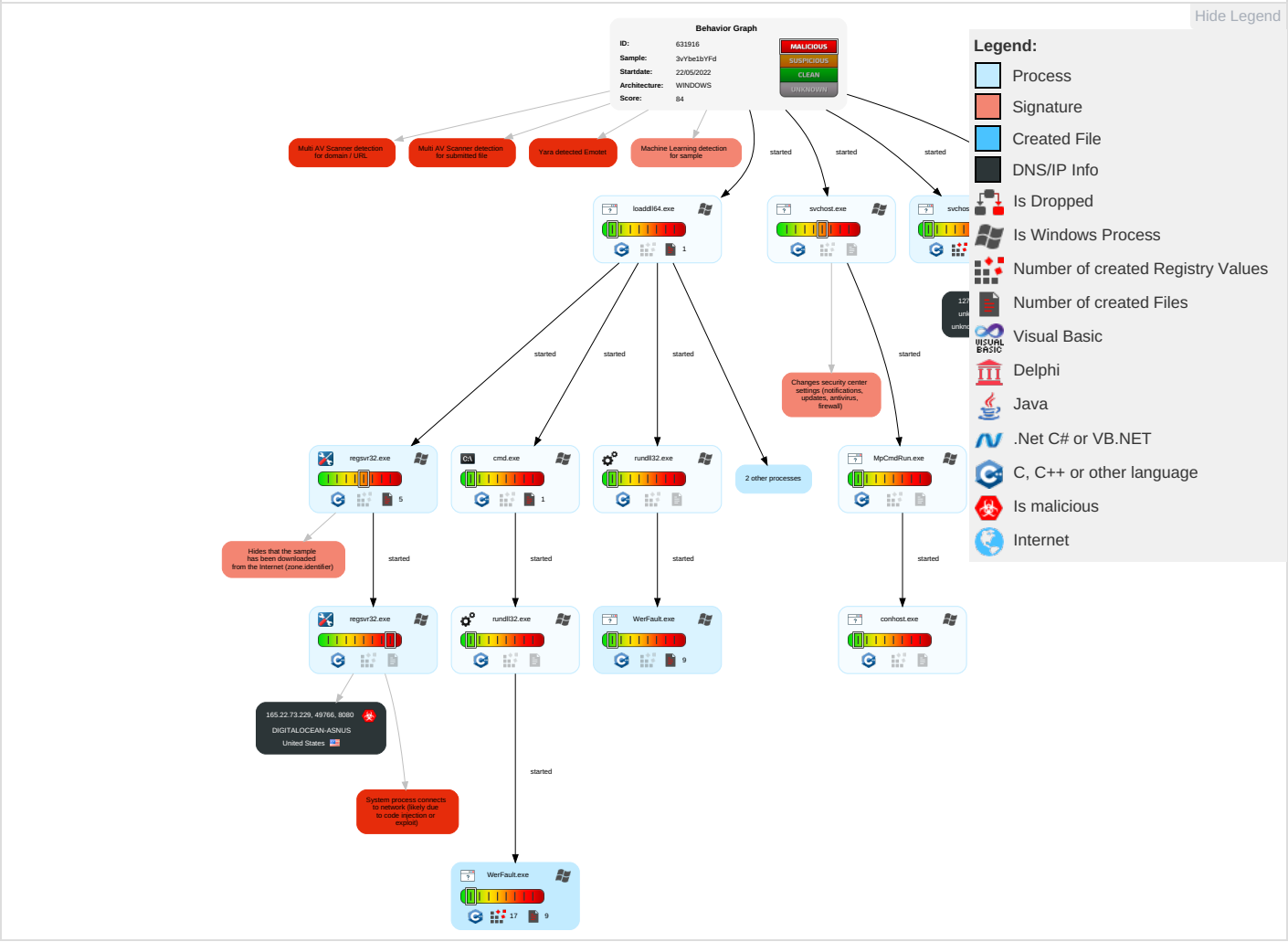
Yara detected Emotet

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

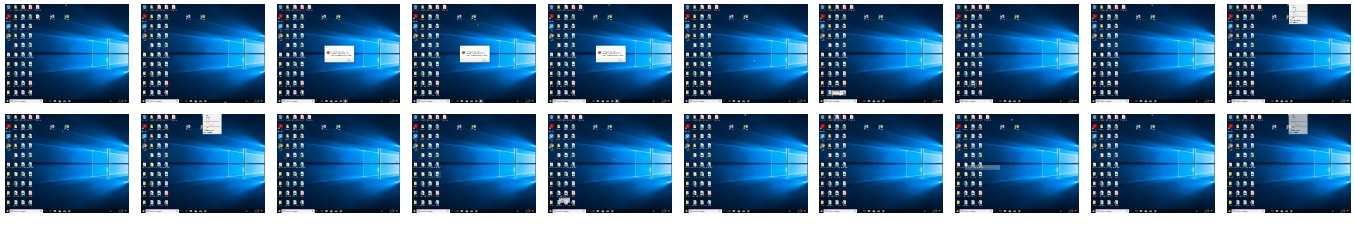
Behavior Graph

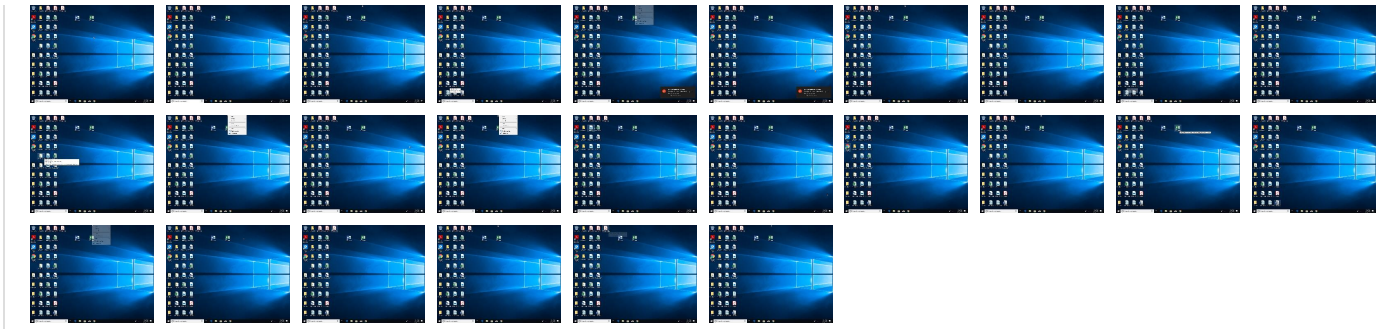


Screenshots

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
3vYbe1bYFd.dll	38%	Virustotal		Browse
3vYbe1bYFd.dll	44%	ReversingLabs	Win64.Trojan.Emotet	
3vYbe1bYFd.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.a80000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.rundll32.exe.1b1ee280000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
7.2.regsvr32.exe.a70000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.0.rundll32.exe.17c4a5c0000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.17c4a5c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.0.rundll32.exe.17c4a5c0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.1b1ee280000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.0.rundll32.exe.1b1ee280000.2.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://165.22.73.229/X)	0%	Avira URL Cloud	safe	
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://165.22.73.229/	7%	Virustotal		Browse
http://https://165.22.73.229/	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://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/	2%	Virustotal		Browse
http://https://165.22.73.229:8080/	0%	Avira URL Cloud	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://165.22.73.229:8080/Num	0%	Avira URL Cloud	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

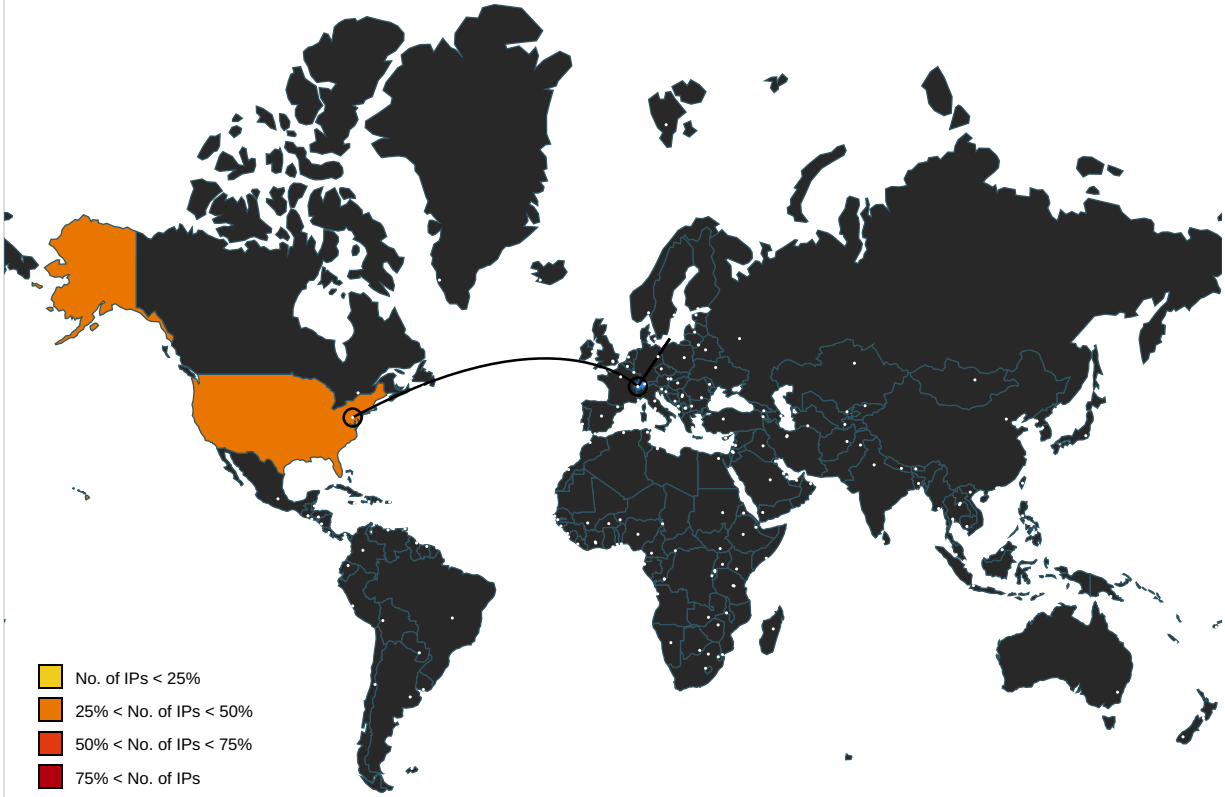
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000013.00000002.312803288.00000221D283D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000013.00000003.312116623.00000221D2861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000013.00000002.312803288.00000221D283D000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000013.00000002.312826926.00000221D285C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312130314.00000221D285A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000013.00000002.312819477.00000221D284D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312166225.00000221D2840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312321754.00000221D2847000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000013.00000003.312116623.00000221D2861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000013.00000003.312513217.00000221D2841000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312166225.00000221D2840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000002.312809233.00000221D2842000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000013.00000003.312116623.00000221D2861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000013.00000003.312130314.00000221D285A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000013.00000003.290171266.00000221D2831000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229/X)	regsvr32.exe, 00000007.00000002.761091751.0000000000C29000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000013.00000003.312513217.00000221D2841000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312166225.00000221D2840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000002.312809233.00000221D2842000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 0000001C.00000003.384563683.00000147C939F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384622362.00000147C93AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384810344.00000147C9819000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384500828.00000147C938D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384683574.00000147C9802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384749517.00000147C93AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384709277.00000147C9803000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 0000001C.00000003.384563683.00000147C939F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384622362.00000147C93AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384810344.00000147C9819000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384500828.00000147C938D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384683574.00000147C9802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384749517.00000147C93AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384709277.00000147C9803000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.tiktok.com/legal/report	svchost.exe, 0000001C.00000003.398457041.00000147C938D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.bingmapsportal.com	svchost.exe, 00000013.00000002.312736884.00000221D2813000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000013.00000003.290171266.00000221D2831000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000002.312803288.00000221D283D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000013.00000003.312116623.00000221D2861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 0000001C.00000003.394204946.00000147C938D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000013.00000003.312506917.00000221D2845000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312166225.00000221D2840000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 00000013.00000002.312840026.00000221D286A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312096480.00000221D2868000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000013.00000002.312803288.00000221D283D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 00000013.00000003.290171266.00000221D2831000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000013.00000003.290171266.00000221D2831000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229/	regsvr32.exe, 00000007.00000002.761091751.0000000000C29000.00000004.00000020.00020000.00000000.sdmp	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000013.00000002.312826926.00000221D285C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312166225.00000221D2840000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312130314.00000221D285A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 0000001C.00000003.398467391.00000147C939E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.398457041.00000147C938D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.398437784.00000147C93B4000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.398490535.00000147C9802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.398416500.00000147C93B4000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000013.00000002.312736884.00000221D2813000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000002.312803288.00000221D283D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000011.00000002.761224539.000002507823F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000013.00000003.312116623.00000221D2861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000013.00000003.290171266.00000221D2831000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000013.00000003.312116623.00000221D2861000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.hotspotshield.com/	svchost.exe, 0000001C.00000003.384563683.00000147C939F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384622362.00000147C93AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384810344.00000147C9819000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384500828.00000147C938D000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384683574.00000147C9802000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384749517.00000147C93AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000001C.00000003.384709277.00000147C9803000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000013.00000002.312826926.00000221D285C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312130314.00000221D285A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 0000001C.00000003.394204946.00000147C938D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000013.00000002.312826926.00000221D285C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312130314.00000221D285A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000013.00000003.312107116.00000221D2864000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000013.00000003.312116623.00000221D2861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229:8080/	regsvr32.exe, 00000007.00000003.540254415.0000000000C75000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.761091751.0000000000C29000.00000004.00000020.00020000.00000000.sdmp	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://disneyplus.com/legal.	svchost.exe, 0000001C.00000003.394204946.00000147C938D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000013.00000002.312797567.00000221D283A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.290171266.00000221D2831000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://165.22.73.229:8080/Num	regsvr32.exe, 00000007.00000002.761149209.0000000000C31000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.540193804.0000000000C31000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000013.00000002.312826926.00000221D285C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312130314.00000221D285A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000011.00000002.761224539.000002507823F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000013.00000003.312116623.00000221D2861000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 0000001C.00000003.394204946.00000147C938D000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000011.00000002.761224539.000002507823F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000013.00000002.312826926.00000221D285C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000013.00000003.312130314.00000221D285A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000013.00000003.312130314.00000221D285A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

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

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	631916
Start date and time: 22/05/202223:30:10	2022-05-22 23:30:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3vYbe1bYFd (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:	38
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: 73% (good quality ratio 38.9%) • Quality average: 32.7% • Quality standard deviation: 37.6%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 173.222.108.226, 173.222.108.210, 52.182.143.212, 20.189.173.22, 23.211.4.86, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, onedsblobprdwus17.westus.cloudapp.azure.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dspw65.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, onedsblobprdcus15.centralus.cloudapp.azure.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:31:53	API Interceptor	2x Sleep call for process: WerFault.exe modified
23:31:53	API Interceptor	11x Sleep call for process: svchost.exe modified
23:32:42	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):	0.24944566632166001
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4x:BJiRdwfu2SRU4x
MD5:	B7710F04CD26EF3089B00D65792B7EB6
SHA1:	69734098B1235A1E445810FAFCB1A686B68651B7
SHA-256:	741703B76F674114A583F439723F5C16A77C9641A80BC5FAE361A78900B29C42
SHA-512:	B1C917EF3E3E2C9512753B2184B4B7C61AA67684F0876389160AE7DCD641E7F4372795DCD5058E2490769C718EF4F844AB6A445639C22F200CCB6EA2731A2D64
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 0x1bb4a119, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25071801024438184
Encrypted:	false
SSDEEP:	384:qTv+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:qTkSB2nSB2RSjlK/+mLesOj1J2
MD5:	E14FAE95EE90CAD8C79F8107A74428C8
SHA1:	71FC246327F6C63CEB46C6B127C536CAB7EBB5F0
SHA-256:	39075249A3AA81E4546AAC47FCA7EE29EDED549AAEB4DB13EF6C78DE14FA2689
SHA-512:	6870F5C6311365693B0BDDB61416D5C8B7675B2FCC9840A24CE3A39DE88348EE51E9A2C2D99750232B83C244C7022A6E413DA51133C5906DD8CB920377CE56C
Malicious:	false
Preview:	....e.f.3...w.....).....#...z..5....z..h.(.....#...z....).....3...w.....B.....@..... ....J..#…z.....#…z..... .....

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

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

File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07666280159075223
Encrypted:	false
SSDEEP:	3:e+/tJ7vQbv5GfcwzgKVGg0tlyJx3f+all3VkttlmlnI:eutJrQbkfGEb3fn3
MD5:	31550EFE7C994CD8F077DD084BC726F7
SHA1:	4421281E7818DB3358201A180B5F0BCE45E53D28
SHA-256:	445AA9630690BDEBF926EF9C2053B20DD5930E19C6F59942DDB2AB0C7464A213
SHA-512:	E23C889614A400AA73E3192C3E3B1EAC43DE33F1B7EEA340A51479F892AC1AF5A9DE46D8223783F3B3F943101EDF0D7207CFC823BBD412FDAB1A5367BF20342 5
Malicious:	false
Preview:	6. p.....3...w..5....z...#...z.....#...z...#...z..@....#...z.....#...z..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_051c2651\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):	0.784968311722452
Encrypted:	false
SSDEEP:	96:GrFUo91riAi3XJPnyqjD55oe7RH6tpXIQcQZc6nfcEtcw3iXaXz+HbHgSQgJPbWS:gZrxinJKlHXjf3UjY9/u7sLS274ltSE
MD5:	1710E9326AFEA9998AF7F497836C5C16
SHA1:	1A7941A771FDDEB4440436BF8310D9B44BC782C5
SHA-256:	1FE11AF8CB7062C6FB709CF82D2D5E572F9321CFFE0B0B20B6430DCF9A1B592E
SHA-512:	8614081171D83616DEDBE4A1A0B021980E6BAA07B780873CD76D89A4CA5ADFBA6EE98C1E83C00B38414125C445F45AB092EAEA618804D23C850D38408108E12 7
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.=.1.3.2.9.7.7.2.8.6.8.0.9.6.0.0.3.5.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.2.8.6.8.2.8.1.9.3.9.9.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.6.a.8.7.f.d.b.-.a.5.4.a.-.4.b.7.8.-.a.8.6.5.-.5.0.9.0.f.2.4.4.f.3.9.6... ..I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.0.0.4.1.5.4.d.-.7.e.6.7.-.4.6.c.3.-.a.7.1.c.-.f.5.2.f.7.3.c.8.c.e.9.1.....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._.3.v.Y.b.e.1.b.Y.F.d...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.=.0.0.0.0.1.1.e.8.-.0.0.0.1.-.0.0.1.c.-.a.0.c.c.-.2.2.4.4.2.3.6.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_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_0f5825e4\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):	0.7838974640996313
Encrypted:	false
SSDEEP:	96:isFYHAiCJPnyRjD55oe7RH6tpXIQcQZc6nfcEtcw3iXaXz+HbHgSQgJPbWIDV9wu:b2giCJK2HXjf3UjY9/u7sLS274ltSE
MD5:	C7EB88A48A2FE09D961F8E917B574E71
SHA1:	C0D44238CC5D08DDBB2FF6A104DE7F7395208EFF
SHA-256:	D6EE637EA5722B70A9D3093ACF10BDF19FA02107A4F789FC720C4DFB5CC0267A
SHA-512:	340262C53DDFF4D72F28215F6345F7788800C92D3D2E8824376E8B214EC760A6CFAC9809DF5522FFF7495F241FF3184B197471EDED3DD4EA4F666F480FED7A13
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.=.1.3.2.9.7.7.2.8.6.8.0.6.8.8.5.0.7.7.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.2.8.6.8.2.2.8.2.2.5.6.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.e.4.b.f.7.c.4.-.3.1.0.d.-.4.8.d.1.-.a.f.5.0.-.f.c.c.3.6.d.d.9.d.6.c.9... ..I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.9.e.3.4.e.e.5.-.7.5.2.0.-.4.7.a.8.-.9.e.8.b.-.b.d.b.a.0.9.a.3.f.0.7.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.3.v.Y.b.e.1.b.Y.F.d...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.=.0.0.0.0.0.1.9.4.-.0.0.0.1.-.0.0.1.c.-.1.a.9.5.-.e.c.4.3.2.3.6.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\WERA615.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun May 22 21:31:21 2022, 0x1205a4 type

Category:	dropped
Size (bytes):	75116
Entropy (8bit):	2.118245558539423
Encrypted:	false
SSDEEP:	384:hS04cSe2YqH2u9ACyZh4TnrUQcldYnt45p05YLLS1VXZ0:hSfMqH2cACyZh4TnrUQ+A45pQtVG
MD5:	B115D6A1B6776E59E85F916FE9C4EA45
SHA1:	61C5313280A21F5AC3EAC330E183D88721705E1A
SHA-256:	AEE44B2AD57C8E9F759FD10F50598711950E91F2ED03E66622775EC47815A219
SHA-512:	883ECE2C30859324B186DA588C8ECCB9B9862A3AC2D2B65A8139EE16E7B21A10938E9138F79BB9B4ABCA2BB928C8C890F36C796F9388C93DB9E0246D31FDC4B8
Malicious:	false
Preview:	MDMP..... .....b.....h.....T...d@.....`.....8.....T.....".....$.....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\WERA72E.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun May 22 21:31:21 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64208
Entropy (8bit):	2.3136211856774245
Encrypted:	false
SSDEEP:	384:d304cSe2YqH2XC45PcldYnt7VExfIPNGGG1:d3fMqH2XC45P+AJ/Pz
MD5:	517F6F23A8845C8D8765F0E55CB40661
SHA1:	70B715C6390B0B7FFC8239E9CC72956A0069171A
SHA-256:	64905E3C3A58AF00508C183DF7307EB6763BE3910632A63603EC4891F1A14C2A
SHA-512:	D038DC2C1BA737704FF19E0FB815574A24ACD08B0602FFB10E0F3DF2EE5EC14B3AFB1D6495E8E49189622A80DC7EFB1AC4C761193719D205E513FEF3FE7D320
Malicious:	false
Preview:	MDMP..... .....b.....8.....$...d;.....`.....8.....T.....X...x.....".....$.....U.....B.....P%... ...Lw.....G...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\WERA933.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8646
Entropy (8bit):	3.7004507622257856
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi2MikTa8R6Y0nfEegmfYMQS98L+prW89bX4zaf5/dm:RrlsNigkTa8R6YMfEegmfYMQS98AXcaq
MD5:	FB9E0DE5504A1A99BDE0234D95D8D884
SHA1:	D91BD5668C17A5955453BBD35BC0C92DBCC0B43E
SHA-256:	1FA65A38DA8408EFB2DD015667AA3C02B7B9100A0564B344BA6795ECACAAA5CD
SHA-512:	CFFA4B3288FA47D52E0F06D6314924C37D89F1ABF77A95CB6C4DA35F0C18DD656AE91DDC881290FE895259FCF3189375F25965F7F16E85DECAD2223F7A1C86AF
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.0.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA8C.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):	4.501735967996476

Encrypted:	false
SSDEEP:	48:cvIwSD8zsAtJgtBI9UxAZWgc8sqYjf8fm8M4JC6jC6KDnFxyq8vh6KDiZESC5Snd:uITfAHCxAogrsqYwJ9BQWUhVvnd
MD5:	5DAA47139205F365B6E8914DE9D1898B
SHA1:	462ACE3F69D4874370070D2A78D4E7D497EB631E
SHA-256:	4DBB9CB279B0D987D2DB16E45144EA32E881DB358755CB80A1070D22DB2BFFEB
SHA-512:	1227EF356819ECF524224D617BFD7E15434001C087561542C4286E907014F2CF92BDAA07E7702D1236CCCBD3E1DA191AF8C5FB728019CFAB9A3C4DF321DC870
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="1526802" />.. <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\WERAB17.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):	8644
Entropy (8bit):	3.6998664781983086
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi45+bafsu6Y8CmgmfYMQS98L+prA89bcGzafb0m:RrlsNi++baEu6YRmgmfYMQS98icSafN
MD5:	BFCD5E77D95580D5A1564D82090E0B0A
SHA1:	6F667BD1884F9887DAE945E0C23444DFA81E3714
SHA-256:	21AF07C9B56E13A5F7906354B676CB4A2CFC8A5C8A7B01025E07676C61FB7C65
SHA-512:	62D02E5172976B026DD20F1E642DB6BCC36ED05798C732A14F33AFAB154DD2B125A38C7D334A388FEA7464F4BF94131412AEEAB6B0B6DF640DE0DCCE44153C11
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.5.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERACDD.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):	4.501696655393521
Encrypted:	false
SSDEEP:	48:cvIwSD8zsAtJgtBI9UxAZWgc8sqYjQ8fm8M4JC6jC6KDnFNrT/yq8vh6KDDzZESw:uITfAHCxAogrsqYJJ9BMXWUEzVv6d
MD5:	E551E5C460AE3F9AE4DDCE5E9C33F4EC
SHA1:	0440A6D03E58B1D3EC486CA2879602AAF534799A
SHA-256:	6D617A5E6BB4FE81BA492567D3A504A74BF436314E73D8652809CB3780F67903
SHA-512:	4802BED87AB8F152601E4E9FB54E19F0F061F7CF185A966C9C211604F444789EA1894122B7B7984FAB34A4F6B6651181EEAF4E798E66088DC758FE8D28C9F5F6
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="1526802" />.. <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....(.......,..................l........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...~$..>......s.I.S....~1..IV.2Ri:..]R!8...q...I.X.%.)@......2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....z..| .#.......I...

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	330
Entropy (8bit):	3.120848828934212
Encrypted:	false
SSDEEP:	6:kKLECoJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:zFkPlE99SNxAhUesE1
MD5:	BB79A36E412519C31F2FA1E15559EE8E
SHA1:	B975FB80D29D1E910A6EDC67ADA2D8CE67916D24
SHA-256:	0ABCB20EB4F94CDAB0C702D5CEC63996FC3EC9D84A2E43850C2B8174B27F2B43
SHA-512:	765DDF20F95264993BFC68F94645FFB813EC731D11AF54F72498ABC690EC2F194041D3665048F26A164838466C988E9718FB7B5D8FA502F5A345DD686CD5F1E3
Malicious:	false
Preview:	p...... ....k.X#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):	3.1611207443073126
Encrypted:	false
SSDEEP:	192:cY+38+DJM+i2Jt+iDQ+yw+f0+rU+0Jtk+EOtF+E7tC+Ewb+g:j+s+i+Z+z+B+c+Y+0g+J+j+v+g
MD5:	E72F80A2B350441B88816D8B1B5FB862
SHA1:	AA9C335C0A960F72E319840C5BEF1D315B288174
SHA-256:	F0C346E9B34F224257FBECE95A777C3D59E7043D72A65D684472E8DBEBC19C12
SHA-512:	A585076248FEEFFF0BA325192B8B9ECEF443C8091DE47CB706A1CCFD4F49A58D284D45240885C22359826841FCB1DAD6DDB7BFE1A18B46F53342FC377C55A3 6
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):	7.152740840989443
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:	3vYbe1bYFd.dll
File size:	371200
MD5:	bf2f633fde70f181cc81fe6dffb048e7
SHA1:	b3aedb0275ec4f55f21a2e672e87c96b36f38959
SHA256:	663127c151c31915e66da770d7e2109306f1e2bf12acce04bb3defcb0de92134
SHA512:	c44fd444e946228a5892cead87ef9a79c2ab6f0b47205ca6bd34728b561920e805330f9c6d2ccc8917555e6deb2e785c1615f0427fa78001326260b53bef883e
SSDEEP:	6144:hlNuuXQASByX7RxoJcXy16qFHJ7wwD1w3pq6jTK/V9OT0u:hlNu9ASByX7jy/BJ7rGTK/V3
TLSH:	D9848E46F7F551E5E8F7C13889A23267F9317C948B38A7CB8A44466A4F70BA0E93D701
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....8..ik..ik..ik...k..ik...k..ik...k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich..ik.....PE..d....{.b....."

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

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

Entrypoint Preview

Instruction
dec esp
mov dword ptr [esp+18h], eax
mov dword ptr [esp+10h], edx
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 28h
cmp dword ptr [esp+38h], 01h
jne 00007FDC589B5187h

Instruction
call 00007FDC589BA4E7h
dec esp
mov eax, dword ptr [esp+40h]
mov edx, dword ptr [esp+38h]
dec eax
mov ecx, dword ptr [esp+30h]
call 00007FDC589B5194h
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 00007FDC589B5192h
cmp dword ptr [00028DE8h], 00000000h
jne 00007FDC589B5189h
xor eax, eax
jmp 00007FDC589B52A4h
cmp dword ptr [esp+58h], 01h
je 00007FDC589B5189h
cmp dword ptr [esp+58h], 02h
jne 00007FDC589B51D0h
dec eax
cmp dword ptr [0001ED99h], 00000000h
je 00007FDC589B519Ah
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call dword ptr [0001ED83h]
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
je 00007FDC589B5199h
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call 00007FDC589B4EEAh
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
jne 00007FDC589B5189h

Instruction
xor eax, eax

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2aab0	0x84	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2a1e4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x30000	0x2e9fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x2f000	0xfcc	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5f000	0x294	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x22000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x203fa	0x20400	False	0.405439983043	zlib compressed data	5.75409030586	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x22000	0x8b34	0x8c00	False	0.275474330357	data	4.41578795519	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2b000	0x3798	0x1400	False	0.161328125	data	2.21550179132	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x2f000	0xfcc	0x1000	False	0.5048828125	data	5.08183440168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x30000	0x2e9fc	0x2ea00	False	0.887011980563	data	7.85049584102	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5f000	0x6fc	0x800	False	0.21435546875	data	2.34217115221	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

DLL	Import

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	

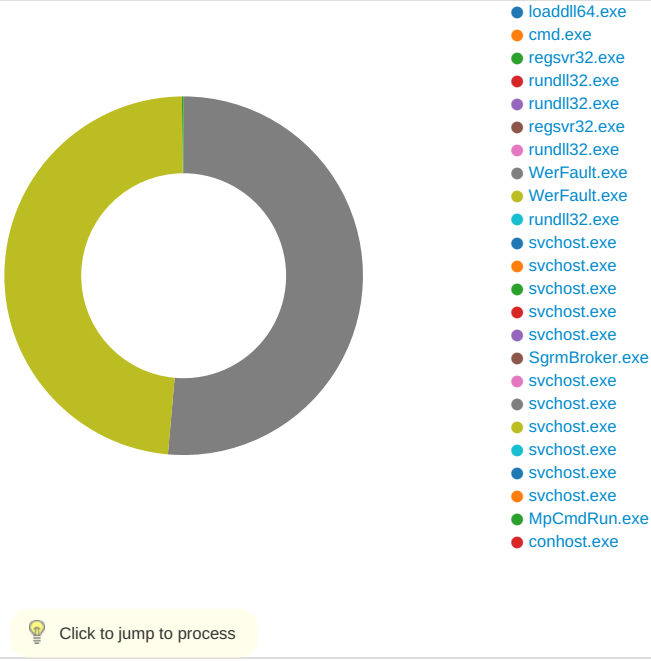
Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 23:31:47.009109020 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:31:47.051754951 CEST	8080	49766	165.22.73.229	192.168.2.4
May 22, 2022 23:31:47.052501917 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:31:47.091161013 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:31:47.133675098 CEST	8080	49766	165.22.73.229	192.168.2.4
May 22, 2022 23:31:47.143002033 CEST	8080	49766	165.22.73.229	192.168.2.4
May 22, 2022 23:31:47.143063068 CEST	8080	49766	165.22.73.229	192.168.2.4
May 22, 2022 23:31:47.143141985 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:31:47.143212080 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:31:52.041250944 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:31:52.084741116 CEST	8080	49766	165.22.73.229	192.168.2.4
May 22, 2022 23:31:52.087090969 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:31:52.089977026 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:31:52.173083067 CEST	8080	49766	165.22.73.229	192.168.2.4
May 22, 2022 23:31:52.451834917 CEST	8080	49766	165.22.73.229	192.168.2.4
May 22, 2022 23:31:52.452003002 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:31:55.452534914 CEST	8080	49766	165.22.73.229	192.168.2.4
May 22, 2022 23:31:55.452583075 CEST	8080	49766	165.22.73.229	192.168.2.4
May 22, 2022 23:31:55.452686071 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:33:37.179620028 CEST	49766	8080	192.168.2.4	165.22.73.229
May 22, 2022 23:33:37.179672956 CEST	49766	8080	192.168.2.4	165.22.73.229

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **3196**, Parent PID: **4604**

General

Target ID:	0
Start time:	23:31:14
Start date:	22/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll"
Imagebase:	0x7ff663f80000
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: **5828**, Parent PID: **3196**

General

Target ID:	1
Start time:	23:31:14
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\3vYbe1bYFd.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: 480, Parent PID: 3196

General

Target ID:	2
Start time:	23:31:15
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\3vYbe1bYFd.dll
Imagebase:	0x7ff71d2d0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.246249403.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.245868285.0000000000A80000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 404, Parent PID: 5828

General

Target ID:	3
Start time:	23:31:15
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\3vYbe1bYFd.dll",#1
Imagebase:	0x7ff77e580000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.245653456.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.244009564.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.318869549.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.318986135.000001B1EE280000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.245946166.000001B1EE280000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.244126583.000001B1EE280000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **4584**, Parent PID: **3196**

General

Target ID:	4
Start time:	23:31:15
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,AddIn_FileTime
Imagebase:	0x7ff77e580000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.319251227.0000017C4A5C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.246074508.0000017C4A5C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.245943775.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.244143793.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.319155462.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.244338347.0000017C4A5C0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **4140**, Parent PID: **480**

General

Target ID:	7
Start time:	23:31:18
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\ZhCaZiQILulll\dyxOJP.dll"
Imagebase:	0x7ff71d2d0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.761554390.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.760699536.0000000000A70000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **1260**, Parent PID: **3196**

General

Target ID:	8
Start time:	23:31:18
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,AddIn_SystemTime
Imagebase:	0x7ff77e580000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WerFault.exe PID: **3896**, Parent PID: **404**

General

Target ID:	9
Start time:	23:31:20
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 404 -s 336
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\WERA615.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.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\WERA933.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\WERA933.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\WERAA8C.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\WERAA8C.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_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_0f5825e4	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_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_0f5825e4\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\WERA615.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA8C.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA8C.tmp.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC8FC.tmp.csv	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERC90D.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\WERA615.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	9600	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\WERA615.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 fd 25 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 fd 5d fd 01 00 00 54 05 00 00 fd 03 00 00 fd 01 00 00 fd fd 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]Tb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	10324	1232	3c 00 0e 00 00 00 00 00 fd 0b fd fd 01 00 00 00 00 58 7e 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 06 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 42 fd fd 6e 00 00 00 00 58 7e fd 7f 00 00 00 00 58 7e fd 7f 00 00 00 00 58 7e fd 7f 00 00 08 fd fd fd fd 00 00 00 fd fd fd fd fd 00 00 00 3c 00 0e 00 00 00 00 00 fd fd fd fd fd 00 00 00 14 53 12 fd 01 00 00 0a 00 00 00 00 00 00 00 28 22 fd fd fd 0f 00 00 fd fd fd fd fd fd fd fd fd 52 12 fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1d 13 fd 01 00 00 fd 00 00 00 00 00 00	<X~_3++S++SBnX~X~X ~<S("R	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	1632	168	1c 06 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 54 28 00 00	T(	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	16484	20	55 00 00 00 00 fd 02 fd 01 00 00 00 00 06 00 00 00 fd 45 00 00	UE	success or wait	85	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	17848	6	01 04 01 00 04 22	"	success or wait	84	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	60356	9416	fd 57 fd fd fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 85 fd 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	WH	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	1800	4	04 00 00 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	11556	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 00 fd fd fd fd fd fd fd fd fd fd fd fd fd 38 f6 fd fd 00 00 00 fd fd fd fd fd fd fd 38 f6 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 76 fd fd 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 38 f6 fd fd 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++F888	success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	1948	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 85 fd 00 00 00 68 fd 50 00 00 00 fd 05 00 00 24 fd 00 00 fd 04 00 00 fd 3b 00 00	ph$;	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	2008	4	19 00 00 00		success or wait	25	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	9606	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\WERA615.tmp.dmp	4604	4344	00 00 5d fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 3a 28 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 53 01 00 00 04 00 00 00 fd fd fd 02 fd 7f 00 00 fd fd fd 02 fd 7f 00 00 00 00 03 fd 01 00 00 00 fd 59 fd 45 23 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 01 00 00 00 00 00	]<2|h+:(BB?#`A pSYE#nS	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	8956	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 33 02 00 00 00 00 00 fd 0e 03 00 00 00 00 48 56 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 76 fd 03 00 00 00 00 00 73 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 25 1b 00 00 00 00 00 63 fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 05 06 00 00 00 00 00 6a fd fd 3b 00 00 00 00 20 fd fd 1f 00 00 00 00 fd 2f fd 22 00 00 00 00 fd fd 0d 01 00 00 00 00 fd 3e 01 00 fd 09 01 00 fd fd 05 00 fd fd 0a 00 63 fd 04 00 06 7f 15 00 fd 05 06 00 6e 2e 00 fd fd 01 00 73 52 13 00 00 00 00 00 b5 1b 00 15 54 04 00 44 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 05 00	ZbHVvs%c@j; /">c.sRTD	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA615.tmp.dmp	69772	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\WERA615.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 68 12 00 00 05 00 00 00 54 05 00 00 64 40 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0d 00 00 fd 17 01 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	hTd@`8T"$	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	964	28	3c 00 50 00 69 00 64 00 3e 00 34 00 30 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>404</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	992	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	996	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1000	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\WERA933.tmp.WERInternalMetadata.xml	1070	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1074	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1078	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1168	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1172	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1176	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 34 00 39 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6493</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1218	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1222	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1226	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\WERA933.tmp.WERInternalMetadata.xml	1304	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1308	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\WERA933.tmp.WERInternalMetadata.xml	1312	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\WERA933.tmp.WERInternalMetadata.xml	1364	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1368	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1372	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\WERA933.tmp.WERInternalMetadata.xml	1416	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1420	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1426	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 34 00 33 00 36 00 31 00 34 00 37 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 04361472 </PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1522	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1526	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1532	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 36 00 39 00 35 00 32 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>2203408695296</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1612	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1616	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1622	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 33 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>26316</PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1698	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1702	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\WERA933.tmp.WERInternalMetadata.xml	1708	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 33 00 33 00 37 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>105033728</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1808	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1812	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1818	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 31 00 31 00 34 00 37 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>7114752</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1898	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1902	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	1908	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>106552</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2022	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2026	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2032	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>106352</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2130	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2134	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\WERA933.tmp.WERInternalMetadata.xml	2140	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 39 00 32 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21928</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2264	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2268	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2274	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 35 00 37 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21576</QuotaNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2382	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2386	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2392	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 39 00 31 00 32 00 38 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>1912832</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2468	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2472	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2478	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 35 00 33 00 39 00 38 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101539840</PeakPagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2574	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2578	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\WERA933.tmp.WERInternalMetadata.xml	2584	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 39 00 31 00 32 00 38 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>1912832</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2656	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2660	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2664	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\WERA933.tmp.WERInternalMetadata.xml	2710	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2714	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2718	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\WERA933.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2758	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\WERA933.tmp.WERInternalMetadata.xml	2798	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2802	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2810	30	3c 00 50 00 69 00 64 00 3e 00 35 00 38 00 32 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5828</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2840	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2844	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2852	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\WERA933.tmp.WERInternalMetadata.xml	2912	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	2916	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\WERA933.tmp.WERInternalMetadata.xml	2924	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\WERA933.tmp.WERInternalMetadata.xml	3014	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3018	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3026	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 38 00 39 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6892</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3068	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3072	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3080	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\WERA933.tmp.WERInternalMetadata.xml	3158	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3162	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3170	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\WERA933.tmp.WERInternalMetadata.xml	3222	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3226	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3234	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\WERA933.tmp.WERInternalMetadata.xml	3278	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3282	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\WERA933.tmp.WERInternalMetadata.xml	3292	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>22033 70369024 </PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3388	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3392	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3402	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>220337036 9024</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3482	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3486	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3496	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\WERA933.tmp.WERInternalMetadata.xml	3568	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3572	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3582	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 39 00 33 00 36 00 38 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2 936832</P eakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3678	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3682	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3692	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 39 00 33 00 36 00 38 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>29368 32</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3772	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\WERA933.tmp.WERInternalMetadata.xml	3776	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3786	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>27840</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3898	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3902	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	3912	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>27664</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4008	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4012	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4022	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>4208</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4144	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4148	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4158	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\WERA933.tmp.WERInternalMetadata.xml	4264	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\WERA933.tmp.WERInternalMetadata.xml	4268	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4278	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 34 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3149824</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4368	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\WERA933.tmp.WERInternalMetadata.xml	4460	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4464	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4474	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 34 00 39 00 38 00 32 00 34 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3149824</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4546	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4550	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	4604	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4608	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	4656	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4660	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	4696	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4700	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	4744	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4748	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	4788	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4792	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	4852	4	0d 00 0a 00		success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	4856	2	09 00		success or wait	18	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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 33 00 76 00 59 00 62 00 65 00 31 00 62 00 59 00 46 00 64 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_3vYbe 1bYFd.dll</Parameter0>	success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	5646	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	5650	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	5692	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	5696	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	5736	4	0d 00 0a 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	5740	2	09 00		success or wait	12	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	6298	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	6302	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	6344	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	6348	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	6388	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	6392	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	6490	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	6494	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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 6a 00 74 00 67 00 68 00 69 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>jtghiq, Inc.</SystemManufacturer>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	6608	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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 6a 00 74 00 67 00 68 00 69 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>jtghiq7,1</SystemProductName>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	6708	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	6712	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	6836	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	6840	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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 35 00 39 00 34 00 32 00 36 00 33 00 39 00 37 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>1594263975</OSInstallDate>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	6926	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	6930	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	7036	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	7114	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7118	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	7160	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7164	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	7200	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7204	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	7304	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7308	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	7346	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7350	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	7376	4	0d 00 0a 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	7630	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7634	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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\WERA933.tmp.WERInternalMetadata.xml	7662	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7666	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.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 31 00 3a 00 33 00 31 00 3a 00 32 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-22T21:31:21Z">	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7768	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7772	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	7776	260	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 34 00 30 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 30 00 37 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 30 00 37 00 38 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 00 31	<Process AsId="415" PID="404" UptimeMS="3078" TimeSinceCreationMS="3078" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8036	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8040	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\WERA933.tmp.WERInternalMetadata.xml	8046	182	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 36 00 31 00 35 00 32 00 31 00 39 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="6152192" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8228	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8232	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8236	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8256	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8260	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8262	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8300	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8304	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8306	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8344	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8348	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8352	98	3c 00 47 00 75 00 69 00 64 00 3e 00 30 00 65 00 34 00 62 00 66 00 37 00 63 00 34 00 2d 00 33 00 31 00 30 00 64 00 2d 00 34 00 38 00 64 00 31 00 2d 00 61 00 66 00 35 00 30 00 2d 00 66 00 63 00 63 00 33 00 36 00 64 00 64 00 39 00 64 00 36 00 63 00 39 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>0e4bf7c4-310d-48d1-af50-fcc36dd9d6c9</Guid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8450	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8454	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\WERA933.tmp.WERInternalMetadata.xml	8458	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 32 00 54 00 32 00 31 00 3a 00 33 00 31 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-05-22T21:31:21Z</CreationTime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8556	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8560	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8562	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8602	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA933.tmp.WERInternalMetadata.xml	8606	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAA8C.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_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_0f5825e4\Report.wer	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_0f5825e4\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_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_0f5825e4\Report.wer	9582	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 38 00 34 00 32 00 30 00 38 00 35 00 31 00 39 00 32 00	MetadataHash=842085192	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: WerFault.exe PID: **1404**, Parent PID: **4584**

General

Target ID:	10
Start time:	23:31:20
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 4584 -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\WERA72E.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\WERA72E.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\WERAB17.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\WERAB17.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\WERACDD.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\WERACDD.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_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_051c2651	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_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_051c2651\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\WERA72E.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACDD.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERACDD.tmp.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCAD3.tmp.csv	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCAF3.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\WERA72E.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 fd fd fd 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	9552	6	00 00 00 00 00 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 50 25 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 fd fd 47 01 00 00 54 05 00 00 fd 03 00 00 fd 11 00 00 fd fd 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	UBP%LwGTb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	10276	1232	3c 2f 46 fd 3f fd 00 00 40 14 5d fd fd 7f 00 00 00 00 58 7e fd 7f 00 00 7d 45 fd 02 fd 7f 00 00 64 00 0e 00 00 00 00 00 fd 0b fd 4b 7c 01 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 06 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 54 fd fd 56 6e 00 00 00 00 58 7e fd 7f 00 00 00 00 58 7e fd 7f 00 00 00 00 58 7e fd 7f 00 00 68 fd 5f 76 00 00 00 fd fd 5f 76 00 00 00 64 00 0e 00 00 00 00 00 38 fd 5f 76 00 00 00 58 5b 5f 4a 7c 01 00 00 0a 00 00 00 00 00 00 00 28 22 fd fd fd 0f 00 00 fd fd fd fd fd fd fd fd 5a 5f 4a 7c 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 10 60 4a 7c 01 00 00 fd 00 00 00 00 00 00	</F? @]X~}EdK|_3++S++TVn X~X~X~hvvd8vX[_J| ("Z_J|`J|	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	1632	168	fd 0c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 24 28 00 00	$(	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	15204	20	52 00 00 00 00 fd 02 fd 01 00 00 00 06 00 00 00 fd 40 00 00	R@	success or wait	82	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	16520	6	01 04 01 00 04 22	"	success or wait	81	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	56116	2856	76 fd fd 02 fd 7f 00 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 18 fd 5f 76 00 00 00 11 fd 5f 76 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 fd fd fd 76 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 41 5f 4a 7c 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 5f 4a 7c 01 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	v`2vvvA_J|/_J|PP	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	11508	1232	fd fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 78 fd 5f 76 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 78 fd 5f 76 00 00 00 fd fd fd fd fd fd fd fd 78 fd 5f 76 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 5f 76 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 78 fd 5f 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 02 fd 7f 00	xv 3++S++Fxvxvvxv	success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	1900	48	fd 16 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 00 fd fd 76 00 00 00 fd fd 5f 76 00 00 00 28 07 00 00 fd 4a 00 00 fd 04 00 00 fd 36 00 00	vv(J6	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	9558	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	4556	4344	00 00 5d fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 0a 28 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 53 01 00 00 04 00 00 00 fd fd fd 02 fd 7f 00 00 fd fd fd 02 fd 7f 00 00 00 00 03 fd 01 00 00 00 61 0b fd 45 23 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 53 01 00 00 00 00 00	]<2|h+(BB?#`A pSaE#nS	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	8908	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 34 02 00 00 00 00 00 fd 0e 03 00 00 00 00 5a 56 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 9e 03 00 00 00 00 00 73 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 47 19 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd 05 06 00 00 00 00 00 3a fd 0f 3c 00 00 00 00 20 fd fd 1f 00 00 00 00 36 5e fd 22 00 00 00 00 17 7c 0e 01 00 00 00 00 fd 3e 01 00 48 0c 01 00 23 05 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd 05 06 00 fd 20 2f 00 fd fd 01 00 fd 76 13 00 00 00 00 00 18 09 1c 00 79 54 04 00 62 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 05 00	ZbZVsG@:< 6^"|>H /vyTb	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERA72E.tmp.dmp	58972	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\WERA72E.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 fd 10 00 00 38 12 00 00 05 00 00 00 24 05 00 00 64 3b 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 58 0d 00 00 78 fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	8$d;`8TXx"$	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 34 00 35 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4584</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.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\WERAB17.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 36 00 36 00 31 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>6612</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1228	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1314	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1374	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1428	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 35 00 30 00 33 00 37 00 39 00 36 00 32 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>2203503796224</PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1534	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 34 00 30 00 38 00 31 00 37 00 31 00 30 00 30 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203408171008</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1624	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 32 00 38 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>26286</PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1710	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 30 00 30 00 39 00 31 00 35 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>105009152</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1820	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 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\WERAB17.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	1910	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 35 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>106552</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2028	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\WERAB17.tmp.WERInternalMetadata.xml	2034	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 36 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>106352</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2136	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2142	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 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\WERAB17.tmp.WERInternalMetadata.xml	2266	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2270	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2276	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 31 00 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\WERAB17.tmp.WERInternalMetadata.xml	2384	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2388	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2394	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 32 00 36 00 38 00 31 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1826816</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2474	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\WERAB17.tmp.WERInternalMetadata.xml	2480	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 31 00 34 00 35 00 33 00 38 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101453824</PeakPagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2586	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 38 00 32 00 36 00 38 00 31 00 36 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1826816</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2666	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2720	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2760	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3196</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2846	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\WERAB17.tmp.WERInternalMetadata.xml	2854	72	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 61 00 64 00 64 00 6c 00 6c 00 36 00 34 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>loaddll64.exe</ImageName>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2926	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2930	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	2938	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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\WERAB17.tmp.WERInternalMetadata.xml	3028	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3032	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3040	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 37 00 39 00 31 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7791</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3082	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3086	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3094	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3172	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3176	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3184	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3236	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3240	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3248	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3292	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3296	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3306	90	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 34 00 35 00 31 00 31 00 34 00 36 00 32 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>4345114624</PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3396	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3400	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3410	74	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 34 00 33 00 34 00 31 00 31 00 34 00 39 00 36 00 39 00 36 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>4341149696</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3498	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 36 00 34 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>641</PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3584	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 33 00 31 00 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\WERAB17.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3684	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\WERAB17.tmp.WERInternalMetadata.xml	3694	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 39 00 37 00 38 00 35 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>2297856</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3774	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3788	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 38 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>28208</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3900	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3904	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	3914	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 30 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 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\WERAB17.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4024	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 30 00 37 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>4072</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4146	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4150	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\WERAB17.tmp.WERInternalMetadata.xml	4160	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>2984</QuotaNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4280	74	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 39 00 32 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>479232</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4368	90	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 37 00 34 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>487424</PeakPagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4458	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4462	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4472	70	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 37 00 39 00 32 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>479232</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4542	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4546	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4554	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4600	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4604	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\WERAB17.tmp.WERInternalMetadata.xml	4610	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4652	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4656	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4660	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4692	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4696	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4698	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4746	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4784	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4788	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4792	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX64</EventType>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4848	4	0d 00 0a 00		success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4852	2	09 00		success or wait	18	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	4856	104	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 33 00 76 00 59 00 62 00 65 00 31 00 62 00 59 00 46 00 64 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_3vYbe 1bYFd.dll</Parameter0>	success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	5642	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	5646	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\WERAB17.tmp.WERInternalMetadata.xml	5648	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	5688	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	5692	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	5694	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	5732	4	0d 00 0a 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	5736	2	09 00		success or wait	12	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	5740	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6300	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6340	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6344	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6346	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6384	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6388	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6392	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6486	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6490	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\WERAB17.tmp.WERInternalMetadata.xml	6494	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 6a 00 74 00 67 00 68 00 69 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>jtghiq, Inc.</SystemManufacturer>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6600	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6604	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6608	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 6a 00 74 00 67 00 68 00 69 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>jtghiq7,1</SystemProductName>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6704	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6708	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6712	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6840	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 35 00 39 00 34 00 32 00 36 00 33 00 39 00 37 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>1594263975</OSInstallDate>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6922	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	6926	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\WERAB17.tmp.WERInternalMetadata.xml	6930	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7032	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7036	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7040	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\WERAB17.tmp.WERInternalMetadata.xml	7110	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7114	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7116	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\WERAB17.tmp.WERInternalMetadata.xml	7156	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7160	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7162	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\WERAB17.tmp.WERInternalMetadata.xml	7196	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7200	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7204	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\WERAB17.tmp.WERInternalMetadata.xml	7300	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7304	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7306	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\WERAB17.tmp.WERInternalMetadata.xml	7342	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7346	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7348	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\WERAB17.tmp.WERInternalMetadata.xml	7372	4	0d 00 0a 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7376	2	09 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7380	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\WERAB17.tmp.WERInternalMetadata.xml	7626	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7630	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7632	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\WERAB17.tmp.WERInternalMetadata.xml	7658	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7662	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7664	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 31 00 3a 00 33 00 31 00 3a 00 32 00 32 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-22T21:31:22Z">	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7764	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	7768	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\WERAB17.tmp.WERInternalMetadata.xml	7772	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 31 00 36 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 34 00 35 00 38 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 38 00 32 00 38 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 32 00 38 00 32 00 38 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="4584" UptimeMS="2828" TimeSinceCreationMS="2828" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8034	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8038	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8044	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 31 00 35 00 32 00 31 00 39 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="6152192" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8226	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8230	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8234	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\WERAB17.tmp.WERInternalMetadata.xml	8254	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8258	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8260	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\WERAB17.tmp.WERInternalMetadata.xml	8298	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8302	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8304	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\WERAB17.tmp.WERInternalMetadata.xml	8342	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8346	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8350	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 36 00 61 00 38 00 37 00 66 00 64 00 62 00 2d 00 61 00 35 00 34 00 61 00 2d 00 34 00 62 00 37 00 38 00 2d 00 61 00 38 00 36 00 35 00 2d 00 35 00 30 00 39 00 30 00 66 00 32 00 34 00 34 00 66 00 33 00 39 00 36 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>86a87fdb-a54a-4b78-a865-5090f244f396</Guid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8448	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8452	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8456	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 31 00 3a 00 33 00 31 00 3a 00 32 00 32 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>2022-05-22T21:31:22Z</CreationTime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8554	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8558	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8560	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\WERAB17.tmp.WERInternalMetadata.xml	8600	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB17.tmp.WERInternalMetadata.xml	8604	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\WERACDD.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 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 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 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_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_051c2651\Report.wer	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_051c2651\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_3vY_f2377edc972ec1548b57729b7c19e6e09b2f3f_e0906090_051c2651\Report.wer	9582	44	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 33 00 35 00 36 00 31 00 36 00 35 00 30 00 32 00 39 00	MetadataHash=356165029	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\{fda3240c-d1cc-5f2b-a779-3b62ecae2519}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFFEFA51D2D	unknown
\REGISTRY\A\{fda3240c-d1cc-5f2b-a779-3b62ecae2519}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFFEFA51D2D	unknown
\REGISTRY\A\{fda3240c-d1cc-5f2b-a779-3b62ecae2519}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFFEFA2E3FE	unknown

Analysis Process: rundll32.exe PID: **6020**, Parent PID: **3196**

General

Target ID:	13
Start time:	23:31:22
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3vYbe1bYFd.dll,DllRegisterServer
Imagebase:	0x7ff77e580000
File size:	69632 bytes

MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6476**, Parent PID: **564**

General

Target ID:	15
Start time:	23:31:33
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
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: svchost.exe PID: **6520**, Parent PID: **564**

General

Target ID:	16
Start time:	23:31:38
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: **6560**, Parent PID: **564**

General

Target ID:	17
Start time:	23:31:38
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: **6628**, Parent PID: **564**

General

Target ID:	18
Start time:	23:31:39
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: **6668**, Parent PID: **564**

General

Target ID:	19
Start time:	23:31:40
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: **6732**, Parent PID: **564**

General	
Target ID:	20
Start time:	23:31:40
Start date:	22/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff651bf0000
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: **6780**, Parent PID: **564**

General	
Target ID:	22
Start time:	23:31:41
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: **6896**, Parent PID: **564**

General	
Target ID:	23
Start time:	23:31:41
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: **7052**, Parent PID: **564**

General

Target ID:	24
Start time:	23:31:44
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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **6220**, Parent PID: **564**

General

Target ID:	25
Start time:	23:31:52
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: svchost.exe PID: **1012**, Parent PID: **564**

General

Target ID:	26
Start time:	23:32:03
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	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

Analysis Process: svchost.exe PID: **6292**, Parent PID: **564**

General

Target ID:	28
Start time:	23:32:16
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: MpCmdRun.exe PID: **1348**, Parent PID: **6780**

General

Target ID:	33
Start time:	23:32:41
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

Analysis Process: conhost.exe PID: **3108**, Parent PID: **1348**

General	
Target ID:	34
Start time:	23:32:42
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

Disassembly

No disassembly