ID: 631909
Sample Name: qJhkILqiEA.dll
Cookbook: default.jbs
Time: 22:47:18
Date: 22/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

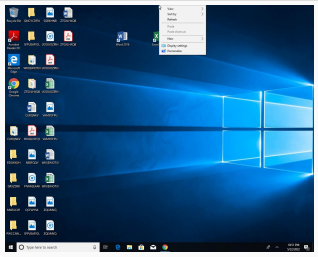
Windows Analysis Report

qJhkILqiEA.dll

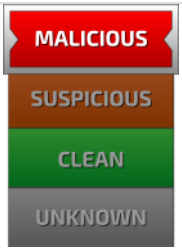
Overview

General Information

Sample Name:	qJhkILqiEA.dll
Analysis ID:	631909
MD5:	8516983eedc869..
SHA1:	bdd250044234e5.
SHA256:	90498f1ee590da..
Tags:	exe trojan
Infos:	



Detection



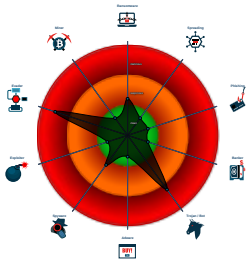
Emotet

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 3696 cmdline: loaddll64.exe "C:\Users\user\Desktop\qJhkILqiEA.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 3024 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\qJhkILqiEA.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 3180 cmdline: rundll32.exe "C:\Users\user\Desktop\qJhkILqiEA.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 4364 cmdline: C:\Windows\system32\WerFault.exe -u -p 3180 -s 336 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - regsvr32.exe (PID: 3080 cmdline: regsvr32.exe /s C:\Users\user\Desktop\qJhkILqiEA.dll MD5: D78B75FC68247E8A63ACBA846182740E)
      - regsvr32.exe (PID: 1908 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IxbPFgKevemZDIDo\xuHXDLB.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
    - rundll32.exe (PID: 3088 cmdline: rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,AddIn_FileTime MD5: 73C519F050C20580F8A62C849D49215A)
      - WerFault.exe (PID: 3392 cmdline: C:\Windows\system32\WerFault.exe -u -p 3088 -s 332 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
    - rundll32.exe (PID: 1860 cmdline: rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,AddIn_SystemTime MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 1192 cmdline: rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
- svchost.exe (PID: 6576 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6616 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6680 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6716 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6788 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6836 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 2956 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 5008 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6972 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7136 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5752 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6560 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6964 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5112 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.245516131.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000000.247075589.00000298CA850000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.327804102.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.248215300.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000002.00000002.248087583.0000000000750000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.750000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.0.rundll32.exe.1b300000000.2.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.rundll32.exe.298ca850000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1b300000000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1b300000000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

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

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

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

HIPS / PFW / Operating System Protection Evasion

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

Lowering of HIPS / PFW / Operating System Security Settings

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

Stealing of Sensitive Information

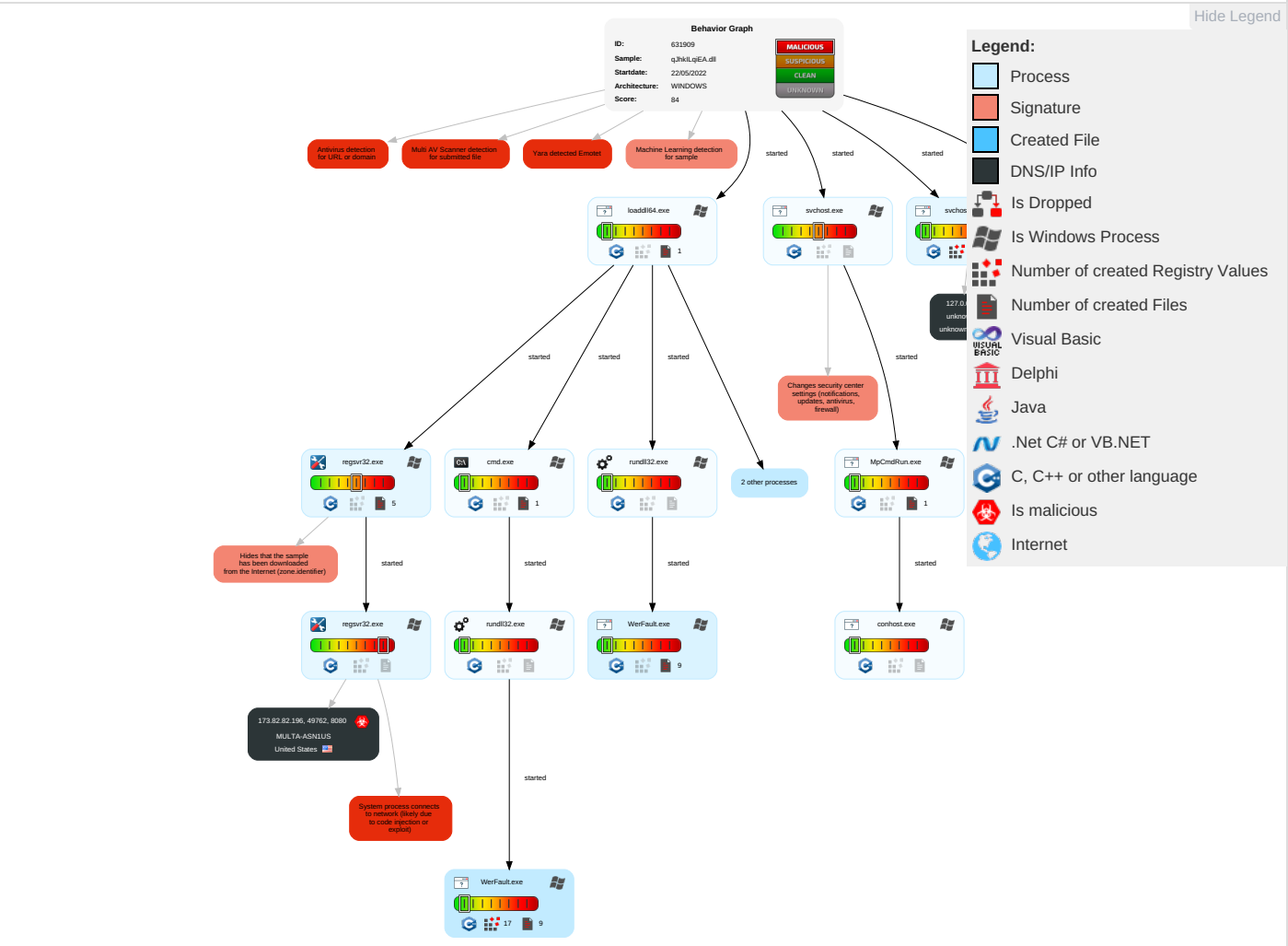
Yara detected Emotet

Mitre Att&ck Matrix

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

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

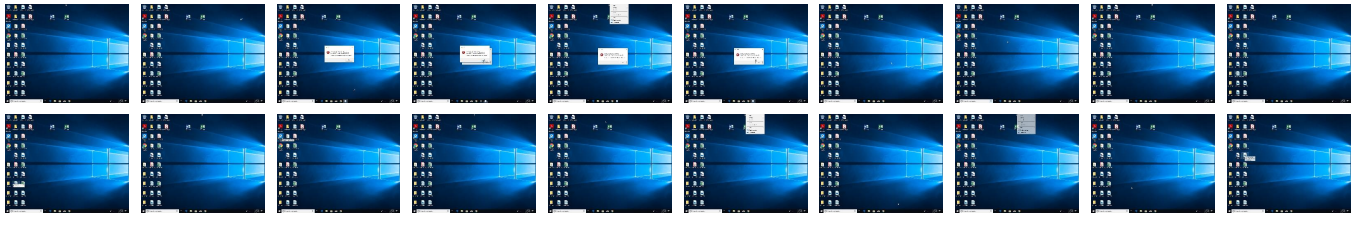
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://173.82.82.196:8080/f	100%	Avira URL Cloud	malware	
http://https://173.82.82.196/0.v9	100%	Avira URL Cloud	malware	
http://https://www.pango.co/privacy	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/(.	100%	Avira URL Cloud	malware	
http://https://173.82.82.196/	100%	URL Reputation	malware	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/	100%	URL Reputation	malware	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://173.82.82.196:8080/P	100%	Avira URL Cloud	malware	

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, 00000012.00000002.317593966.00000195B5E3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000012.00000003.316801953.00000195B5E50000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000012.00000002.317593966.00000195B5E3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 00000012.00000003.316812477.00000195B5E4A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317612674.00000195B5E4C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000012.00000002.317577945.00000195B5E24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000012.00000003.316801953.00000195B5E50000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196:8080/f	regsvr32.exe, 00000007.00000002.647496148.0000000000A7E000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.535348405.0000000000A7E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000012.00000003.316857943.00000195B5E41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.317078891.00000195B5E42000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317608897.00000195B5E43000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000012.00000003.316801953.00000195B5E50000.00000004.00000020.00020000.00000000.sdmp	false		high

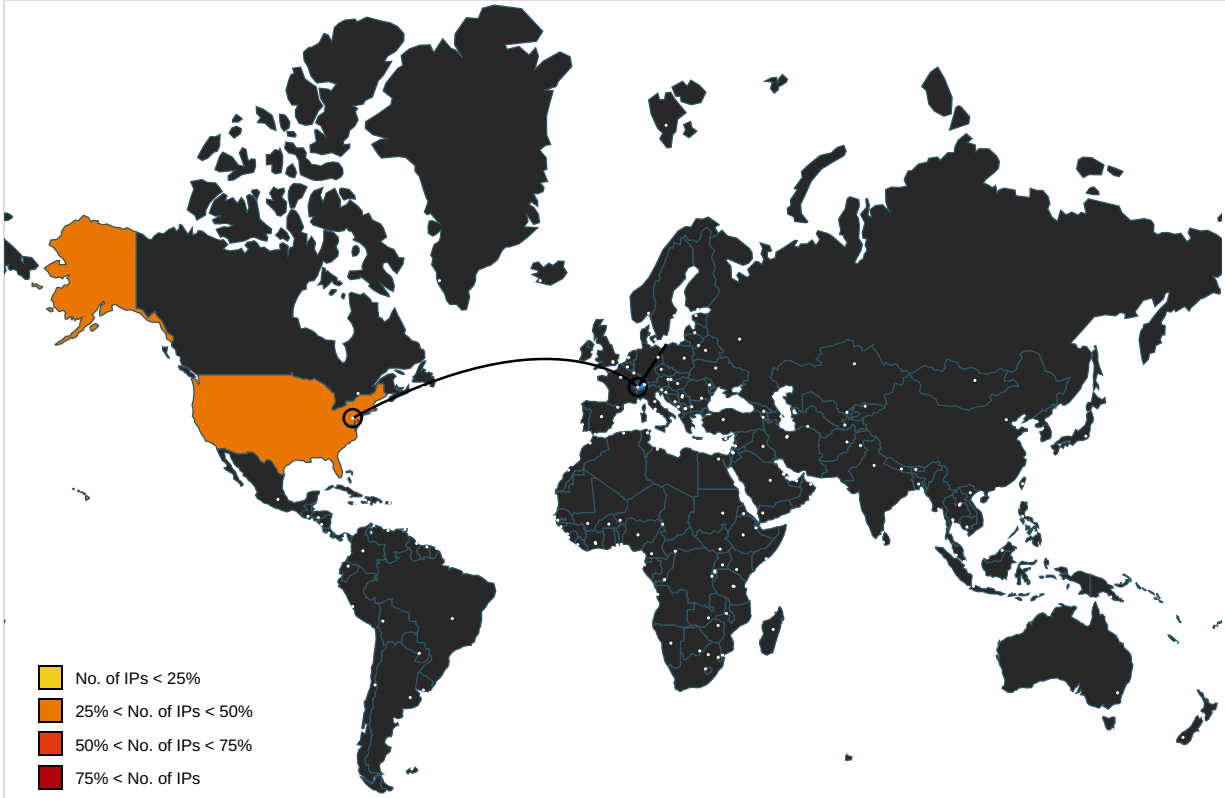
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000012.00000003.316812477.00000195B5E4A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317577945.00000195B5E24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196/0.v9	regsvr32.exe, 00000007.00000002.647445988.0000000000A72000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.535336382.0000000000A72000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000012.00000003.316857943.00000195B5E41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.317078891.00000195B5E42000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317608897.00000195B5E43000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000021.00000003.492529643.000001C77B9A8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492482077.000001C77BE03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492465997.000001C77BE02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492512474.000001C77B986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492397766.000001C77B998000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492570326.000001C77BE19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492430641.000001C77B9A8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000021.00000003.492529643.000001C77B9A8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492482077.000001C77BE03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492465997.000001C77BE02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492512474.000001C77B986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492397766.000001C77B998000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492570326.000001C77BE19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492430641.000001C77B9A8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ecn.dev.virtualearth.net/mapcontrol/roadshield.ashx?bucket=	svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000012.00000002.317577945.00000195B5E24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317577945.00000195B5E24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000012.00000002.317593966.00000195B5E3E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000012.00000003.316801953.00000195B5E50000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000021.00000003.495561358.000001C77B98E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.495361255.000001C77B9A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000012.00000003.316857943.00000195B5E41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.317044423.00000195B5E46000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 00000012.00000003.316702192.00000195B5E68000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317635939.00000195B5E6B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000012.00000002.317593966.00000195B5E3E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 00000012.00000002.317577945.00000195B5E24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196:8080/(.	regsvr32.exe, 00000007.00000002.647445988.0000000000A72000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.535336382.0000000000A72000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196/	regsvr32.exe, 00000007.00000002.647445988.0000000000A72000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.535336382.0000000000A72000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://https://dev.virtualearth.net/REST/v1/Transit/Stops/	svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 00000017.00000002.644662058.0000022F4C213000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000002.523167516.000001C77AEEE000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000012.00000003.316812477.00000195B5E4A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.316857943.00000195B5E41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317612674.00000195B5E4C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000021.00000003.503721537.000001C77BE02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.503700080.000001C77B99F000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.503683010.000001C77B98E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.503649260.000001C77B9B5000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.503617207.000001C77B9B5000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000012.00000002.317593966.00000195B5E3E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317577945.00000195B5E24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000010.00000002.647477108.000001D20863E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000012.00000002.317577945.00000195B5E24000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.316801953.00000195B5E50000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000012.00000003.316801953.00000195B5E50000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000021.00000003.492529643.000001C77B9A8000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492482077.000001C77BE03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492465997.000001C77BE02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492512474.000001C77B986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492397766.000001C77B998000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492570326.000001C77BE19000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.492430641.000001C77B9A8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://173.82.82.196:8080/	regsvr32.exe, 00000007.00000002.647496148.0000000000A7E000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.647895703.0000000000AA4000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.535348405.0000000000A7E000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.536554846.0000000000AA4000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: malware	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000012.00000003.316812477.00000195B5E4A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317612674.00000195B5E4C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000021.00000003.495561358.000001C77B98E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.495361255.000001C77B9A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000012.00000003.316812477.00000195B5E4A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317612674.00000195B5E4C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000012.00000002.317577945.00000195B5E24000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317608897.00000195B5E43000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000012.00000003.316801953.00000195B5E50000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://disneyplus.com/legal.	svchost.exe, 00000021.00000003.495561358.000001C77B98E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.495361255.000001C77B9A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000012.00000003.317228227.00000195B5E3A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000003.291687958.00000195B5E30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000012.00000003.316812477.00000195B5E4A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317612674.00000195B5E4C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000010.00000002.647477108.000001D20863E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000012.00000003.316801953.00000195B5E50000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://help.disneyplus.com.	svchost.exe, 00000021.00000003.495561358.000001C77B98E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000021.00000003.495361255.000001C77B9A0000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000010.00000002.647477108.000001D20863E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://173.82.82.196:8080/P	regsvr32.exe, 00000007.00000002.647895703.0000000000AA4000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.536554846.0000000000AA4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000012.00000003.316812477.00000195B5E4A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000012.00000002.317612674.00000195B5E4C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000012.00000003.316812477.00000195B5E4A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

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

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	631909

Start date and time: 22/05/202222:47:18	2022-05-22 22:47:18 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qJhkILqiEA.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	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: 67.5% (good quality ratio 36%) • Quality average: 32.7% • Quality standard deviation: 37.6%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 173.222.108.210, 173.222.108.226, 20.189.173.22, 52.168.117.173, 104.79.90.110, 20.223.24.244
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, 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, 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
22:49:01	API Interceptor	1x Sleep call for process: svchost.exe modified
22:49:51	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):	0.24943981571860702
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4m:BJiRdwfu2SRU4m
MD5:	D8FF300C6D885188DF2AC60E3BCD71CB
SHA1:	21A25B82AC439052932E64A78951D8F79E5D047A
SHA-256:	B387363557993C28D2FCE0B206954E7F10FDD369168300F4C8749C214BC0DF4B
SHA-512:	4C8AAD83554DF1DA7EF8855B981E7490C97ABC389B0B01D9107DB60505FAAC76D0F9E3EEF6142F960FCBF9F6E85334B40C2C2DE16DD9774372051063162B3E2 D
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 0xe8784526, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.25065638736444334
Encrypted:	false
SSDEEP:	384:8bp+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:8biSB2nSB2RSjlK/+mLesOj1J2
MD5:	7CC246726A494BBEEDDDF2D804264E81
SHA1:	5D8A6E26FDA3D4604503FDEEC2DEE828D27D1907
SHA-256:	CD57CF3B12D5478C28A09E3AC5C81FB79416DA47CF9529A698B162C439A81301
SHA-512:	54B35C130FE2F6C799C6C0366432429629BB7C9A30BE4B68917DDA6E84898E9BB93C40428BBFFD17A4050D070EB7337B34B84BB6BD72391CDE07AB3994166B83
Malicious:	false
Preview:	.xE&... .....e.f.3...w.....).....3...zI..1...z..h.(.....3...zI...).....3...w.....B.....@..... ....k....3...zI.....3...zI..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07689334245217044
Encrypted:	false
SSDEEP:	3:ultlJ7vkUxZW/XbfC4qKpUzXMUgK/Xoll3VkttlmlnI:OlJrkUetn4MN3
MD5:	F16CAFCA17364D171423EA175A7DC2EB
SHA1:	302DF404A45B15292D76BFFBDB5014E842479A4D
SHA-256:	41B9D3515826337015A984E44A842E7394B108406374A0581362B3AFADA93636
SHA-512:	467A7B4B404BA5042B12680CF8CF307A7A117B54651833920F567F1E1AB2B2D2C6AE65EB6EAF06D55C7455DE981EC3961F6160AA1D7033C16746BDCACB649E50
Malicious:	false
Preview:	.....3...w...1...z...3...zI.....3...zI..3...zI..ir.3...z1.....3...zI..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_0d7c99ac\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):	0.78653414067496
Encrypted:	false
SSDEEP:	96:uAFiG6uitmJPnyYjZ55ol7RH6tpXIQcQSc6rcEbcw3dXXaXz+HbHgSQgJPbsIDVx:zvbitmJKeHMvhBjC9/u7sYS274ltY3
MD5:	712C9C534669558E0D3D02502A6D1EBD
SHA1:	2FD4029900005F0D64033CB3AC82E7471FC5E2E3
SHA-256:	E9138AC8E879C912F4DB97F311D1567E848DA56DE387CA61B9A971B668A73209
SHA-512:	844D44C931166904EB83F948AD23B9B7F6B4C432B2F6F56581F1F449E57AFB03B4CCE746147B493D2A2D4293A0EF1E836E979523B4983B0DA5F6B3FDDAB6AF4D
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.=.1.3.2.9.7.7.2.6.1.1.0.3.4.6.2.8.1.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.7.2.6.1.1.2.3.9.2.0.4.3.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.5.d.6.5.e.c.5.-.9.b.f.c.-.4.1.8.c.-.b.a.e.d.-.7.6.f.a.0.9.b.c.5.4.b.b...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.=.7.5.e.e.4.8.c.5.-.c.d.e.3.-.4.5.7.f.-.a.a.a.3.-.9.f.6.c.8.9.7.0.5.8.f.9.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.q.J.h.k.I.L.q.i.E.A...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.c.1.0.-.0.0.0.1.-.0.0.1.c.-.c.8.e.8.-.4.8.4.7.1.d.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_1130994e\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):	0.785382983774044
Encrypted:	false
SSDEEP:	96:3WxFiuinJPnyHjZ55ol7RH6tpXIQcQSc6rcEbcw3dXXaXz+HbHgSQgJPbsIDV9wE:khinJKpHMvhBjC9/u7sYS274ltY3
MD5:	F7E90A1BBDB0CD4F72B29E3908A6C190
SHA1:	60DD6FCDEB84671E399818282F1A73CEF379B5C3
SHA-256:	DCB5344170BEDABEB85285397BB188D7E7AD0CF820316386F05D502FF43C64B9
SHA-512:	953E132C5C402D49F68566C76F96659186BA5B585C19B60DC7B37AF2997DB1DAE392A998B1E496A863889B9DDC3D8FF5E80C020D21F77D5B533382B2A36228F
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.=.1.3.2.9.7.7.2.6.1.0.9.7.5.3.0.1.9.7.....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.=.1.3.2.9.7.7.2.6.1.1.1.9.0.9.2.6.2.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.6.f.a.d.f.5.6.-.2.f.5.8.-.4.9.e.a.-.b.f.4.8.-.8.4.2.0.c.f.c.0.4.f.a.2...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.=.6.3.9.c.0.2.a.7.-.4.3.a.d.-.4.4.5.d.-.8.2.7.f.-.4.c.4.a.4.9.3.e.4.3.c.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e._.q.J.h.k.I.L.q.i.E.A...d.l.l.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.c.6.c.-.0.0.0.1.-.0.0.1.c.-.c.1.9.4.-.1.3.4.7.1.d.6.e.d.8.0.1.....T.a.r.g.e.t.A.p.p.l.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\WER125C.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):	8650
Entropy (8bit):	3.7034582406311083
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiv3VKnrg6YmxagmfWISVOS+prS89bpE/f0Wjm:RrlsNifVKnrg6YoagmfWISIpkfW
MD5:	1046F0EED316DBAFE38CB0D9A0D3CB78
SHA1:	938364FAAD0A8A464AEDC915AB3487F890F7F1E6
SHA-256:	C9685DB4A4BB1C84458EEC1FCF9414DAFE6F793C71D9ECF2CDADF3D9B334A553
SHA-512:	7782873C2DA8E01099F46543676B6DBC2D5D542B607D570BB34084FE9D7A51D8C3EB36AEA0BDBCECBA1BD11108D77328B63D60114C7C8B82A538E82FB0A8B544
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.1.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1422.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):	4.512441673681485
Encrypted:	false
SSDEEP:	48:cvIwSD8zsTrJgtBI9GAK9kWgc8sqYj58fm8M4JCGCZgnFoYVyq8vhZgskZESC5SH:uITfR56grsqYyJ+YVWfkVvpd
MD5:	187432A1D31ED3C938791AFF2B2AFA45
SHA1:	B9F31E06E9E100148B87A03679B02D460A53E9DA
SHA-256:	2B8101185AE6B83AFB966FC5FB1082424A7B5A6CD4397315D79CB0F97496EA30
SHA-512:	E811D8C23F9769E6CE253B1865B081770711500758F19E24060E9ED1C540A791BF2DBEEDE072480D929380A5A1A21C1C694DE1746DDEA2FEA4FD7EC086C6BCD
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="1526759" />.. <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\WER146F.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):	3.7050788967044714
Encrypted:	false
SSDEEP:	192:RrI7r3GLNiefGnn7D6Y7U4igmfWISVOS+prp89bpK/fsjm:RrlsNieGnn7D6Yo/gmfWISVpafV
MD5:	CFE3F6B219A74B629B6621046E8344C0
SHA1:	997AF685CA3C5481E5228D017E6AAC8944032A19
SHA-256:	AAA2FCD607AC304FAC850FE70D38F20A5789396B13D0E1B09F8B6A7FED0171B5
SHA-512:	2B43CC3212A6E457B4AF488CD021607AC0CF78119F5B55CBE4499E2447C9B4BE85CD8A79C1EE0BE7B42560F300A9149A4366D0110D6CD78C0983733BDBFF6F B
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8. 0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>. X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.3.0.8. 8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1664.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):	4.513366664364022
Encrypted:	false
SSDEEP:	48:cvIwSD8zsTrJgtBI9GAK9kWgc8sqYjpT8fm8M4JCGCZgnFOyq8vhZgwfZESC5SMd:uITfR56grsqYSJwWPfVvMd
MD5:	D733CE4203C0A165D35770F1552C8902
SHA1:	1D972A278E1456DC34792310D673B013D31AAC21
SHA-256:	382BD0E26D6BE879B3D019491ECAA6F6CEA0665D542598F560EEBA9587E73248
SHA-512:	5469D506E0499ECA5F1AC7729129D95B8EF6083E6836F3A7D2881DD6CEFED6A16CE8B23F05A9ECC1CBC68ABE522D1CDDFAA1AE1E977D9A34600F9BA4C470 F97
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="1526759" />.. <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\WERD79.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun May 22 20:48:30 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	66002
Entropy (8bit):	2.2680221089329433
Encrypted:	false
SSDEEP:	384:OJMriPwsv7faw5C+mhNNiJkl0niFWxdw+O:ofPNvz75C+mhDibS6dg
MD5:	A9DCC66453173D9D26F7633B9E86B633
SHA1:	870EB92173E26CE8D5DAA00C9105A16FA49B86FC
SHA-256:	200D24DF6B12A1F022C9D578AE06F9B855699AD6A7D994DACE293F2720E9F3CD
SHA-512:	460F505460BDB68BBAF58BC7E2DCA0125FD1C8E40F9AA7BA5391CB66E0278C838D87029770EC166A7D6DC30B9C1FD217B24097AD1C9EF311922F32FDBD094E 49
Malicious:	false
Preview:	MDMP..... .....b.....8.....p;.....`.....8.....T.....*.....".....$.....U.....B.....\%... ...Lw.....g...T.....l.....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\WERFCB.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun May 22 20:48:31 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	64598
Entropy (8bit):	2.3001332838422353

Encrypted:	false
SSDEEP:	384:URJMniPwsv7faw4lWC3bEwFniF/bZyyTgOGR6:U3vPNvz74lWC3bLBS/b2U
MD5:	CE0805F60565B06C14AE97418E371D1F
SHA1:	76BDAD64C7576D826733E8020C6E69FE5FC6EB5D
SHA-256:	1F3E378129CE75950E13C1499498CE9AEB48652B17A04B0FBD5EA80DA96D388C
SHA-512:	BF58974226BD3F91468738A9CAE8B80FAA164E284631FB0D69403E932E4CEC79CA07AAC24169A79FAAB42ADA4AD3386215043D61D88B1A705A116473367C967
Malicious:	false
Preview:	MDMP..... .....b.....8.....p;.....`.....8.....T.....X.....".....$.....U.....B.....\%... ...Lw.....x.>...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:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61480 bytes, 1 file
Category:	dropped
Size (bytes):	61480
Entropy (8bit):	**7.9951219482618905**
Encrypted:	**true**
SSDEEP:	1536:kmu7iDG/SCACih0/8uIGantJdjFpTE8lTeNjiXKGgUN:CeGf5gKsG4vdjFpjlYeX9gUN
MD5:	B9F21D8DB36E88831E5352BB82C438B3
SHA1:	4A3C330954F9F65A2F5FD7E55800E46CE228A3E2
SHA-256:	998E0209690A48ED33B79AF30FC13851E3E3416BED97E3679B6030C10CAB361E
SHA-512:	D4A2AC7C14227FBAF8B532398FB69053F0A0D913273F6917027C8CADBBA80113FDBEC20C2A7EB31B7BB57C99F9FDECCF8576BE5F39346D8B564FC72FB16994 76
Malicious:	false
Preview:	MSCF....(.....,.....I.....y.....Tbr .authroot.stl..$..4..CK..<Tk...c_.d....A.K.....Y.f....!.))$7*I.....e..eKT..k....n.3.....S..9.s.....3H.Mh.....qV.=M6.=.4.F.....V:F..]..... B`....Q...c"U.0.n....J.....4.....i7s..:.27...._...+).lE..he.4|.?,...h....7..PA..b.,. .....#1+..o...g.....2n1m...=.....Dp.;..f..ljX.Dx..r<'.1RI3B0<w.D.z..)D|..8<..c+..'XH..K,.Y..d.j.<.A... ....I_lVb[w..rDp...'.....nL....!G.F....f.fX..r.. ?.....v(...L..<.\.Z..g;.>.0v...P .....|...A..(..x...T0.`g...c..7.U?...9.p..a..&..9.....sV..l0..D..fhi..h.F....q...y.....Mq].4..Z.....={L....AS..9.....:.:..... ...+..P.N....EAQ.V. sr.....y.B.`.Efe..8../....$...y-.q.J.....nP...2.Q8...O.....M.@\.>=X....V..z.4.=.@...ws.N.M3.S.c?.....C4]?..\.K.9.....^...CU.....O....X.`....._.gU...*..V.{V6..m ..D.-|.Q.t.7.....9.~....[...I.<e...~$..>.....s.I.S....~1..IV.2Ri:..]R!8...q...I.X.%.)@.....2.gb,t...}..;...@.Z..<q..y..:...e3..cY.we.$....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):	3.1147882228736057
Encrypted:	false
SSDEEP:	6:kKz/lqoJN+SkQlPlEGYRMY9z+4KlDA3RUesJ21:r/WkPlE99SNxAhUesE1
MD5:	0363219B7DEEC845F2D1295ECAD25D12
SHA1:	A891520C6FF13386920F25934CFC8781AD33337B
SHA-256:	E9ADAF25088C4793C72D2E63718FD56E4AF2537B2DA0ECABCDF22EC36D0CA848
SHA-512:	1BD4B6A17F1C6B070FFF97DBCBD2263215C3CA3E43512A4488FE816242A605D4FDD9F6ED50DDF50BF9AEEA6E66EAB823B456983027C66F007611AE738D111C A1
Malicious:	false
Preview:	p..... .....~..[.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:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBACA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

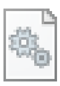
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	10844
Entropy (8bit):	3.1616379606535308
Encrypted:	false
SSDEEP:	192:cY+38+DJM+i2Jt+iDQ+yw+f0+rU+0Jtk+EOtF+E7tC+EwK+V:j+s+i+Z+z+B+c+Y+0g+J+j+2+V
MD5:	6705BF0FB1F764118D7B18E958138FEB
SHA1:	B7D1CD4369B65F74A969674FC2EBC62B1C384494
SHA-256:	1924CCE0EC3F1140F37D9A3B6BF46419F608CF1F8D42AA297A15BA1A879A3129
SHA-512:	0F270A36211EDE11C4E573A56BA72A3BB6733BA2C16D739E14D9368BD7D30F0C5BACABB5EECE9AC85CCAF5555F31FC2D384464E93743C4663CB464C67C01FBAB
Malicious:	false
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-............-.

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	7.158106332990621
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	qJhkILqiEA.dll
File size:	365056
MD5:	8516983eedc8690c1495b828b4262a63
SHA1:	bdd250044234e53e9f08db444a1de00987735930
SHA256:	90498f1ee590da28566434c15efcfd98e829846f233387553ea655fc7559168d
SHA512:	c5b6a37a787a70e70be8614f957c183547b85dfa0913b746f6bc701cec09bd54e04fb53443dfeffedcf83176f581e6a5f4de06219a1fa6d9d015691e9432cd93
SSDEEP:	3072:JI0AM0yQkR9M6lglELtJUNjiWGyWcTb0JUiA2tqZ4IvUlDAj7UOjVifSwHEDQVLK:i5MR9M6y3TWRIvgMSS3AyUrhYu3j
TLSH:	7A747D56F6F110F5E8B7C138C9A23267F8317D559B38A7CB8A08865A4F70BA4E93D740
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........8..ik..ik..ik...k..ik...k..ik...k..ik..hk..ik...k..ik...k..ik...k..ik...k..ikRich..ik................PE..d...v{.b.........."

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180003580
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE

DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x62877B76 [Fri May 20 11:28:54 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	ad5c5b0f3e2e211c551f3b5059e614d7

Entrypoint Preview
Instruction
dec esp
mov dword ptr [esp+18h], eax
mov dword ptr [esp+10h], edx
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 28h
cmp dword ptr [esp+38h], 01h
jne 00007FD70CBF2EE7h
call 00007FD70CBF8247h
dec esp
mov eax, dword ptr [esp+40h]
mov edx, dword ptr [esp+38h]
dec eax
mov ecx, dword ptr [esp+30h]
call 00007FD70CBF2EF4h
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 00007FD70CBF2EF2h
cmp dword ptr [00028DE8h], 00000000h
jne 00007FD70CBF2EE9h
xor eax, eax
jmp 00007FD70CBF3004h
cmp dword ptr [esp+58h], 01h
je 00007FD70CBF2EE9h
cmp dword ptr [esp+58h], 02h

Instruction
jne 00007FD70CBF2F30h
dec eax
cmp dword ptr [0001EDB9h], 00000000h
je 00007FD70CBF2EFAh
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call dword ptr [0001EDA3h]
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
je 00007FD70CBF2EF9h
dec esp
mov eax, dword ptr [esp+60h]
mov edx, dword ptr [esp+58h]
dec eax
mov ecx, dword ptr [esp+50h]
call 00007FD70CBF2C4Ah
mov dword ptr [esp+20h], eax
cmp dword ptr [esp+20h], 00000000h
jne 00007FD70CBF2EE9h
xor eax, eax

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2aad0	0x84	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2a204	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x30000	0x2d1fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x2f000	0xfcc	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5e000	0x294	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x22000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x203fa	0x20400	False	0.405969900678	zlib compressed data	5.75556665875	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x22000	0x8b54	0x8c00	False	0.276395089286	data	4.42213983851	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x2b000	0x3798	0x1400	False	0.1609375	data	2.22442517754	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x2f000	0xfcc	0x1000	False	0.50537109375	data	5.09571430422	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x30000	0x2d1fc	0x2d200	False	0.922572931094	data	7.88663988983	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5e000	0x6f2	0x800	False	0.21337890625	data	2.33584866509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Exports

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

Possible Origin

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

Network Behavior

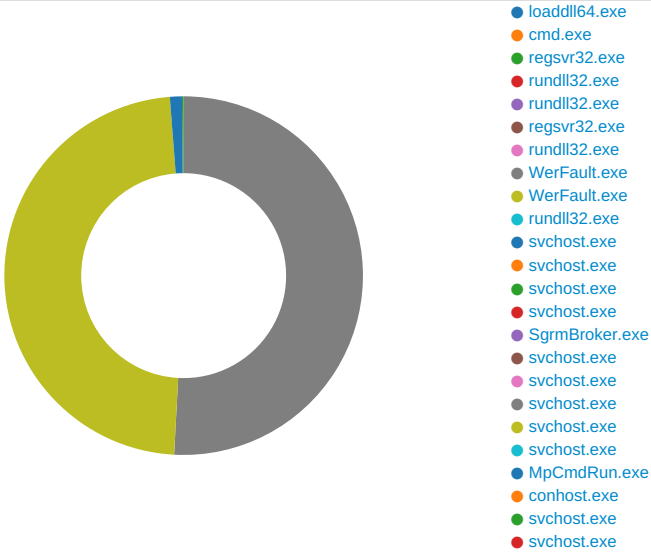
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 22:48:52.333376884 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:48:55.344686031 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:48:55.517919064 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:48:55.518003941 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:48:55.557230949 CEST	49762	8080	192.168.2.4	173.82.82.196

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 22, 2022 22:48:55.730329037 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:48:55.743906021 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:48:55.743937969 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:48:55.743994951 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:48:55.744019032 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:49:01.940469027 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:49:02.113751888 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:49:02.114525080 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:49:02.116019011 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:49:02.131129980 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:49:02.304414034 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:49:02.978549957 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:49:02.980065107 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:49:05.981497049 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:49:05.981561899 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:49:05.981631994 CEST	8080	49762	173.82.82.196	192.168.2.4
May 22, 2022 22:49:05.981753111 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:50:43.110599041 CEST	49762	8080	192.168.2.4	173.82.82.196
May 22, 2022 22:50:43.110629082 CEST	49762	8080	192.168.2.4	173.82.82.196

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **3696**, Parent PID: **2952**

General

Target ID:	0
Start time:	22:48:22
Start date:	22/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\qJhkILqiEA.dll"

Imagebase:	0x7ff7e22b0000
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: 3024, Parent PID: 3696

General

Target ID:	1
Start time:	22:48:23
Start date:	22/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\qJhkILqiEA.dll",#1
Imagebase:	0x7ff7bb450000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 3080, Parent PID: 3696

General

Target ID:	2
Start time:	22:48:23
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\qJhkILqiEA.dll
Imagebase:	0x7ff659710000
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: 00000002.00000002.248215300.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.248087583.0000000000750000.00000040.00001000.00020000.00000000.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\IxbPFgKevemZDIDo\xuHXDLB.dll:Zone.Identifier	success or wait	1	18002AF22	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **3180**, Parent PID: **3024**

General

Target ID:	3
Start time:	22:48:23
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\qJhkILqiEA.dll",#1
Imagebase:	0x7ff65fc10000
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: 00000003.00000000.247075589.00000298CA850000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.327804102.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.245417474.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.327922020.00000298CA850000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.246778578.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000000.245495998.00000298CA850000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: **3088**, Parent PID: **3696**

General

Target ID:	4
Start time:	22:48:23
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,AddIn_FileTime
Imagebase:	0x7ff65fc10000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.245516131.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.328180679.000001B300000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.328137058.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.248564765.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.248656368.000001B300000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000000.245618177.000001B300000000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **1908**, Parent PID: **3080**

General

Target ID:	7
Start time:	22:48:27
Start date:	22/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\IxbPFgKevemZDIDo\xuHXDLB.dll"
Imagebase:	0x7ff659710000
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: 00000007.00000002.646304136.0000000000A00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.648425079.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **1860**, Parent PID: **3696**

General

Target ID:	8
Start time:	22:48:27
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,AddIn_SystemTime
Imagebase:	0x7ff65fc10000
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: **4364**, Parent PID: **3180**

General

Target ID:	9
Start time:	22:48:29
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3180 -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\WERD79.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\WERD79.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\WER125C.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\WER125C.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\WER1422.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\WER1422.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_1130994e	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_1130994e\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\WERD79.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1422.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1422.tmp.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF16.tmp.csv	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERCF56.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\WERD79.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\WERD79.tmp.dmp	9564	6	00 00 00 00 00 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 5c 25 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 fd fd 67 01 00 00 54 05 00 00 fd 03 00 00 6c 0c 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 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\%LwgTlb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	10288	1232	64 01 0a 00 00 00 00 00 fd 0b fd 98 02 00 00 00 00 fd 5f fd 7f 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 fd fd 17 fd fd 6e 00 00 00 00 fd 5f fd 7f 00 00 00 00 fd 5f fd 7f 00 00 00 00 fd 5f fd 7f 00 00 fd fd 56 6f fd 00 00 00 40 fd 56 6f fd 00 00 00 64 01 0a 00 00 00 00 00 fd fd 56 6f fd 00 00 00 14 53 fd 18 02 00 00 0a 00 00 00 00 00 00 00 28 02 fd fd fd 0f 00 00 fd fd fd fd fd fd fd fd 52 fd 18 02 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 11 fd 18 02 00 00 fd 00 00 00 00 00 00	d__3++S++n___Vo@VodVoS(RX	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	1632	168	fd 17 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 30 28 00 00	0(	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	15216	20	5a 00 00 00 68 fd 56 6f fd 00 00 00 08 00 00 00 14 41 00 00	ZhVoA	success or wait	90	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	16660	8	4f 7e fd 02 fd 7f 00 00	O~	success or wait	89	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	57946	2712	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 fd fd fd 6f fd 00 00 00 fd fd fd 6f fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 00 10 67 6f fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 69 fd 18 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 38 30 fd 18 02 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	v`2oogoi80XX	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.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\WERD79.tmp.dmp	11520	1232	00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 56 6f fd 00 00 00 fd fd fd fd fd fd fd fd fd 56 6f 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 68 fd 56 6f fd 00 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 56 6f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 02 fd 7f 00	3++S++FVoVohVoVo	success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	1900	48	60 14 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 60 67 6f fd 00 00 00 68 fd fd 6f fd 00 00 00 fd 0a 00 00 5a fd 00 00 fd 04 00 00 fd 36 00 00	` `gohoZ6	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	9570	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	4556	4356	00 00 5d fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 16 28 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 54 01 00 00 00 00 00 00 fd fd fd 02 fd 7f 00 00 fd fd fd 02 fd 7f 00 00 00 fd 02 fd 01 00 00 00 46 5f fd 48 1d 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 01 00 00 00 00 00	]<2|h+(BB?#`A pTF_HnT	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	8920	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 70 14 03 00 00 00 00 51 54 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd 03 00 00 00 00 00 5f 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 25 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 68 fd fd 36 00 00 00 00 fd 10 fd 1f 00 00 00 00 40 fd fd 22 00 00 00 00 00 fd 78 04 01 00 00 00 00 00 fd 38 01 00 55 09 01 00 fd 76 05 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd fd 05 00 3a fd 2e 00 20 fd 01 00 7b 0e 13 00 00 00 00 00 70 0d 1c 00 7a 52 04 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5e 05 00	ZbpQT%@h6@"x8Uv:. {pzR^	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD79.tmp.dmp	60658	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\WERD79.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 fd 10 00 00 38 12 00 00 05 00 00 00 fd 05 00 00 70 3b 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0d 00 00 2a fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	8p;`8T*"$	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 31 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3180</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 37 00 34 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7749</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1428	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 35 00 30 00 33 00 38 00 31 00 32 00 36 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203503812608</PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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 35 00 30 00 35 00 32 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203408150528</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1624	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 32 00 39 00 37 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>26297</PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1710	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 31 00 37 00 33 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>105017344</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1820	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 30 00 34 00 31 00 30 00 32 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7041024</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>106768</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.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 35 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>106568</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2136	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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 36 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21600</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2266	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2270	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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 32 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21248</QuotaNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2384	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2388	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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 33 00 35 00 30 00 30 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>1835008</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.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 37 00 38 00 34 00 30 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>101478400</PeakPagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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 33 00 35 00 30 00 30 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>1835008</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 33 00 30 00 32 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3024</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	2854	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2914	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2918	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	2926	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3016	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3020	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3028	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 30 00 39 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8092</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3070	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3074	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3082	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3160	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3164	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3172	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3224	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3228	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3236	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3280	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3284	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3294	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203370262528</PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3390	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3394	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3404	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 33 00 37 00 30 00 32 00 36 00 32 00 35 00 32 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203370262528</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3498	72	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 37 00 39 00 32 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>792</PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3584	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 39 00 32 00 30 00 34 00 34 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>2920448</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.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 38 00 30 00 31 00 36 00 36 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2801664</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3774	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3788	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 37 00 38 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>27840</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3900	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	3904	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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 37 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>27664</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4024	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 32 00 30 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>4208</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4146	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.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\WER125C.tmp.WERInternalMetadata.xml	4160	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 36 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>3664</QuotaNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4266	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4280	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 39 00 34 00 31 00 37 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>2994176</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4356	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4360	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4370	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 31 00 34 00 31 00 36 00 33 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>3141632</PeakPagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4462	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4466	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4476	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 39 00 39 00 34 00 31 00 37 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>2994176</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4548	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4552	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4560	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4606	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4610	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\WER125C.tmp.WERInternalMetadata.xml	4616	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4658	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4662	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4666	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4698	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4702	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4704	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4746	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4750	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4752	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4790	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4794	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4798	56	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 42 00 45 00 58 00 36 00 34 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>BEX64</EventType>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4854	4	0d 00 0a 00		success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4858	2	09 00		success or wait	18	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	4862	104	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 5f 00 71 00 4a 00 68 00 6b 00 49 00 4c 00 71 00 69 00 45 00 41 00 2e 00 64 00 6c 00 6c 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe_qJhkI LqiEA.dll</Parameter0>	success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	5648	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	5652	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\WER125C.tmp.WERInternalMetadata.xml	5654	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	5694	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	5698	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	5700	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	5738	4	0d 00 0a 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	5742	2	09 00		success or wait	12	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	5746	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6300	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6304	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6306	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6346	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6350	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6352	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6390	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6394	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6398	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6492	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6496	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\WER125C.tmp.WERInternalMetadata.xml	6500	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 6a 00 76 00 66 00 71 00 68 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>jvfqhq, Inc.</SystemManufacturer>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6606	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6610	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6614	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 6a 00 76 00 66 00 71 00 68 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>jvfqhq7,1</SystemProductName>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6710	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6714	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6718	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6838	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6842	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6846	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 32 00 32 00 32 00 32 00 39 00 38 00 36 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>1612229865</OSInstallDate>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6928	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	6932	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\WER125C.tmp.WERInternalMetadata.xml	6936	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7038	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7042	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7046	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\WER125C.tmp.WERInternalMetadata.xml	7116	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7120	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7122	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\WER125C.tmp.WERInternalMetadata.xml	7162	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7166	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7168	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\WER125C.tmp.WERInternalMetadata.xml	7202	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7206	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7210	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7306	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7310	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7312	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\WER125C.tmp.WERInternalMetadata.xml	7348	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7352	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7354	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\WER125C.tmp.WERInternalMetadata.xml	7378	4	0d 00 0a 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7382	2	09 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7386	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\WER125C.tmp.WERInternalMetadata.xml	7632	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7636	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7638	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\WER125C.tmp.WERInternalMetadata.xml	7664	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7668	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7670	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 32 00 54 00 32 00 30 00 3a 00 34 00 38 00 3a 00 33 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-22T20:48:31Z">	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7770	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	7774	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\WER125C.tmp.WERInternalMetadata.xml	7778	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 33 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 31 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 32 00 33 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 32 00 33 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="413" PID="3180" UptimeMS="3234" TimeSinceCreationMS="3234" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8040	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8044	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8050	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 33 00 38 00 32 00 31 00 35 00 36 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="3821568" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8232	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8236	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8240	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\WER125C.tmp.WERInternalMetadata.xml	8260	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8264	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8266	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\WER125C.tmp.WERInternalMetadata.xml	8304	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8308	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8310	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\WER125C.tmp.WERInternalMetadata.xml	8348	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8352	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8356	98	3c 00 47 00 75 00 69 00 64 00 3e 00 61 00 36 00 66 00 61 00 64 00 66 00 35 00 36 00 2d 00 32 00 66 00 35 00 38 00 2d 00 34 00 39 00 65 00 61 00 2d 00 62 00 66 00 34 00 38 00 2d 00 38 00 34 00 32 00 30 00 63 00 66 00 63 00 30 00 34 00 66 00 61 00 32 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>a6fadf56-2f58-49ea-bf48-8420cfc04fa2</Guid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8454	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8458	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8462	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 35 00 2d 00 32 00 32 00 54 00 32 00 30 00 3a 00 34 00 38 00 3a 00 33 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>2022-05-22T20:48:31Z</CreationTime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8560	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8564	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8566	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\WER125C.tmp.WERInternalMetadata.xml	8606	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER125C.tmp.WERInternalMetadata.xml	8610	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\WER1422.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 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_1130994e\Report.wer	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_1130994e\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	152	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_1130994e\Report.wer	9582	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 35 00 36 00 35 00 37 00 36 00 31 00 38 00 39 00 36 00	MetadataHash=-565761896	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: WerFault.exe PID: **3392**, Parent PID: **3088**

General

Target ID:	10
Start time:	22:48:29
Start date:	22/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 3088 -s 332
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\WERFCB.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\WERFCB.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\WER146F.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\WER146F.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\WER1664.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\WER1664.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_0d7c99ac	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_0d7c99ac\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\WERFCB.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1664.tmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1664.tmp.xml	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD10C.tmp.csv	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERD12D.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\WERFCB.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\WERFCB.tmp.dmp	9564	6	00 00 00 00 00 00		success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	212	1420	09 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 5c 25 00 00 00 01 00 00 4c 77 fd 10 00 00 00 00 00 00 00 00 00 00 00 00 18 01 78 fd 3e 02 00 00 54 05 00 00 fd 03 00 00 10 0c 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\%Lwx>Tb0W. Europe Standard TimeW. Europe Daylight Time	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	10288	1232	fd 3c 14 7b fd 01 00 00 7d 45 fd 02 fd 7f 00 00 00 00 fd 5f fd 7f 00 00 fd 0b 1a 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 06 02 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5f 19 fd fd fd 6e 00 00 00 00 fd 5f fd 7f 00 00 00 00 fd 5f fd 7f 00 00 00 00 fd 5f fd 7f 00 00 fd fd 1b 02 fd 00 00 00 10 fd 1b 02 fd 00 00 00 2e 02 09 00 00 00 00 00 68 fd 1b 02 fd 00 00 00 58 5b 13 7b fd 01 00 00 0a 00 00 00 00 00 00 00 28 02 fd fd fd 0f 00 00 fd fd fd fd fd fd fd fd 5a 13 7b fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 10 14 7b fd 01 00 00 fd 00 00 00 00 00 00	<{}E__3++S++_n___.hX[{(Z{{	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	1632	168	5c 0e 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 30 28 00 00	\0(	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	15216	20	5a 00 00 00 00 fd 02 fd 01 00 00 00 2a 00 00 00 14 41 00 00	Z*A	success or wait	90	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	16660	42	01 14 06 00 14 64 0f 00 14 34 0e 00 14 fd 10 70 01 0a 04 00 0a 34 07 00 0a 32 06 70 01 06 02 00 06 72 02 30 01 04 01 00 04 22	d4p42pr0"	success or wait	89	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	51170	8192	00 00 00 00 00 00 00 00 00 00 50 02 fd 00 00 00 00 40 4f 02 fd 00 00 00 00 00 00 00 00 00 00 00 00 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 3d 02 fd 00 00 00 00 00 00 00 00 00 00 00 10 0c 00 00 00 00 00 00 fd 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3d 02 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	P@OP==	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	1800	4	03 00 00 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	11520	1232	fd fd 1b 02 fd 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1b 02 fd 00 00 00 fd fd fd fd fd fd fd fd fd 1b 02 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 28 fd 1b 02 fd 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1b 02 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 be 02 fd 7f 00	3++S++F(	success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	1900	48	fd 04 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 3d 02 fd 00 00 00 fd fd 4f 02 fd 00 00 00 18 0a 00 00 fd 55 00 00 fd 04 00 00 fd 36 00 00	P=OU6	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	1960	4	19 00 00 00		success or wait	25	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	9570	30	18 00 00 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 00 00	rundll32.exe	success or wait	25	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	4556	4356	00 00 5d fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 16 28 00 00 fd 04 fd fd 00 00 01 00 00 00 0a 00 01 00 fd 42 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 70 00 00 00 0c 00 00 00 01 00 00 00 00 00 00 00 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 54 01 00 00 00 00 00 00 fd fd fd 02 fd 7f 00 00 fd fd fd 02 fd 7f 00 00 00 fd 02 fd 01 00 00 00 24 fd 20 49 1d 6e fd 01 00 10 00 fd 01 00 00 00 fd fd 02 fd 01 00 00 00 00 00 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 01 00 00 00 00 00	]<2|h+(BB?#`A pT$ InT	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	8920	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 70 fd 02 00 00 00 00 00 70 14 03 00 00 00 00 6c 54 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd 03 00 00 00 00 00 5f 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 57 26 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 05 00 00 00 00 00 68 fd fd 36 00 00 00 00 fd 31 fd 1f 00 00 00 00 0d 16 fd 22 00 00 00 00 fd 20 05 01 00 00 00 00 fd 38 01 00 34 0c 01 00 25 7c 05 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd fd 05 00 fd 09 2f 00 39 fd 01 00 75 2b 13 00 00 00 00 00 3f 67 1c 00 fd 52 04 00 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5e 05 00	ZbpplTW&@h61" 84%|/9u+?gR^	success or wait	1	7FFFEFA2E9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	59362	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	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WERFCB.tmp.dmp	32	120	03 00 00 00 fd 00 00 00 08 07 00 00 04 00 00 00 fd 0a 00 00 fd 07 00 00 0d 00 00 00 fd 10 00 00 38 12 00 00 05 00 00 00 fd 05 00 00 70 3b 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 58 0d 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	8p;`8TX"$	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 33 00 30 00 38 00 38 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3088</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 38 00 38 00 32 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7882</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1310	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\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1428	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 35 00 30 00 33 00 38 00 30 00 38 00 35 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>22035 03808512 </PeakVirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 35 00 30 00 35 00 32 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>220340815 0528</VirtualSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1624	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 36 00 32 00 39 00 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>26291 </PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1704	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\WER146F.tmp.WERInternalMetadata.xml	1710	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 31 00 30 00 35 00 30 00 31 00 37 00 33 00 34 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>105017344</PeakWorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 32 00 38 00 37 00 33 00 36 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>7028736</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 37 00 36 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>106768</QuotaPeakPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2028	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 34 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>106344</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2136	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\WER146F.tmp.WERInternalMetadata.xml	2142	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 35 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21536</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2266	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2270	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2276	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 31 00 31 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21184</QuotaNonPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2384	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2388	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2474	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 37 00 30 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101470208</PeakPagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2580	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\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 33 00 36 00 39 00 36 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>3696</Pid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2846	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	2926	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	2930	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\WER146F.tmp.WERInternalMetadata.xml	2938	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3028	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3032	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3040	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 39 00 30 00 37 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>9070</Uptime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3082	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3086	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	3172	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3176	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	3236	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3240	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3292	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3296	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\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	3396	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3400	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	3484	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3488	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 33 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>643</PageFaultCount>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3570	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3574	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	3680	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3684	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3694	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 32 00 33 00 30 00 31 00 39 00 35 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>2301952</WorkingSetSize>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3774	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\WER146F.tmp.WERInternalMetadata.xml	3778	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	3900	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3904	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	3914	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 30 00 34 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>20448</QuotaPagedPoolUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4010	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4014	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	4146	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4150	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	4266	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\WER146F.tmp.WERInternalMetadata.xml	4270	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 38 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>483328</PagefileUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4354	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4358	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	4458	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4462	2	09 00		success or wait	5	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 38 00 33 00 33 00 32 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>483328</PrivateUsage>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4542	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4546	2	09 00		success or wait	4	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	4600	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4604	2	09 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	4652	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4656	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4692	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4696	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	4784	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4788	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	4848	4	0d 00 0a 00		success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	4852	2	09 00		success or wait	18	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 71 00 4a 00 68 00 6b 00 49 00 4c 00 71 00 69 00 45 00 41 00 2e 00 64 00 6c 00 6c 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>rundll32.exe_qJhkl LqiEA.dll</Parameter0>	success or wait	9	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	5642	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	5646	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	5688	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	5692	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	5732	4	0d 00 0a 00		success or wait	6	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	5736	2	09 00		success or wait	12	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	6294	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6298	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	6340	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6344	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	6384	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6388	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	6486	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6490	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 76 00 66 00 71 00 68 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>jvfqhq, Inc.</SystemManufacturer>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6600	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\WER146F.tmp.WERInternalMetadata.xml	6604	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 76 00 66 00 71 00 68 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>jvfqhq7,1</SystemProductName>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6704	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6708	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	6832	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6836	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6840	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 32 00 32 00 32 00 39 00 38 00 36 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>1612229865</OSInstallDate>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6922	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	6926	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	7032	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7036	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\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	7110	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7114	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	7156	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7160	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	7196	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7200	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	7300	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7304	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7342	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7346	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	7372	4	0d 00 0a 00		success or wait	3	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7376	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\WER146F.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 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\WER146F.tmp.WERInternalMetadata.xml	7626	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7630	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	7658	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7662	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 30 00 3a 00 34 00 38 00 3a 00 33 00 31 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-22T20:48:31Z">	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7764	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	7768	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 33 00 30 00 38 00 38 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 33 00 31 00 35 00 36 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 33 00 31 00 35 00 36 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="414" PID="3088" UptimeMS="3156" TimeSinceCreationMS="3156" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8034	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8038	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\WER146F.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 33 00 38 00 32 00 31 00 35 00 36 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="3821568" TimelineUnitShift="12" Timeline="111"/>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8226	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8230	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	8254	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8258	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8298	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8302	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	8342	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8346	2	09 00		success or wait	2	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8350	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 35 00 64 00 36 00 35 00 65 00 63 00 35 00 2d 00 39 00 62 00 66 00 63 00 2d 00 34 00 31 00 38 00 63 00 2d 00 62 00 61 00 65 00 64 00 2d 00 37 00 36 00 66 00 61 00 30 00 39 00 62 00 63 00 35 00 34 00 62 00 62 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>95d65ec5-9bfc-418c-baed-76fa09bc54bb</Guid>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8448	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8452	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\WER146F.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 30 00 3a 00 34 00 38 00 3a 00 33 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>2022-05-22T20:48:31Z</CreationTime>	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8554	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.tmp.WERInternalMetadata.xml	8558	2	09 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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\WER146F.tmp.WERInternalMetadata.xml	8600	4	0d 00 0a 00		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER146F.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
C:\ProgramData\Microsoft\Windows\WER\Temp\WER1664.tmp.xml	0	4892	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_0d7c99ac\Report.wer	0	2	fd fd		success or wait	1	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_0d7c99ac\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	152	7FFFEFA2E9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_qJh_4c633c907b4a85acdb7918fc966c22f420621b1_e567d4a7_0d7c99ac\Report.wer	9582	48	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 31 00 30 00 33 00 33 00 32 00 36 00 34 00 33 00 32 00 37 00	MetadataHash=-1033264327	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\{881459e6-58c9-6320-5502-fa02f11bf79e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFFEFA51D2D	unknown
\REGISTRY\A\{881459e6-58c9-6320-5502-fa02f11bf79e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFFEFA51D2D	unknown
\REGISTRY\A\{881459e6-58c9-6320-5502-fa02f11bf79e}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFFEFA2E3FE	unknown

Analysis Process: rundll32.exe PID: **1192**, Parent PID: **3696**

General

Target ID:	11
Start time:	22:48:31
Start date:	22/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\qJhkILqiEA.dll,DllRegisterServer
Imagebase:	0x7ff65fc10000
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: **6576**, Parent PID: **564**

General

Target ID:	15
Start time:	22:48:46
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
Reputation:	high

Analysis Process: svchost.exe PID: **6616**, Parent PID: **564**

General

Target ID:	16
Start time:	22:48:46
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: **6680**, Parent PID: **564**

General

Target ID:	17
Start time:	22:48:47
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -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: **6716**, Parent PID: **564**

General

Target ID:	18
Start time:	22:48:48
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: **6788**, Parent PID: **564**

General

Target ID:	19
Start time:	22:48:49
Start date:	22/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6353b0000
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: **6836**, Parent PID: **564**

General

Target ID:	20
Start time:	22:48:49
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: **6972**, Parent PID: **564**

General

Target ID:	21
Start time:	22:48:50
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: **7136**, Parent PID: **564**

General

Target ID:	22
Start time:	22:48:55
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: **5752**, Parent PID: **564**

General

Target ID:	23
Start time:	22:49:00
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: **6560**, Parent PID: **564**

General

Target ID:	25
Start time:	22:49:33
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

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: MpCmdRun.exe PID: **2956**, Parent PID: **6836**

General

Target ID:	28
Start time:	22:49:50
Start date:	22/05/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff678970000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	9938	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10120	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 32 00 32 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 32 00 32 00 3a 00 34 00 39 00 3a 00 35 00 31 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sun May 22 2022 22:49:51	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10378	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10464	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10484	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF67899BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10570	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 53 00 75 00 6e 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 32 00 32 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 32 00 32 00 3a 00 34 00 39 00 3a 00 35 00 31 00 0d 00 0a 00	MpCmdRun: End Time: Sun May 22 2022 22:49:51	success or wait	1	7FF67899BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10670	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF67899BC96	WriteFile

Analysis Process: conhost.exe PID: **5008**, Parent PID: **2956**

General

Target ID:	29
Start time:	22:49:51
Start date:	22/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **6964**, Parent PID: **564**

General

Target ID:	31
Start time:	22:49:55
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: **5112**, Parent PID: **564**

General	
Target ID:	33
Start time:	22:50:11
Start date:	22/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff7338d0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly