Recorded Future® Sandbox

Malware Analysis Report

2026-03-03 17:53

Sample ID	260303-v3afzaht5y
Target	WhatsApp Installer (6).exe
SHA256	bb2aff493d76602afe402f40f810afb329c380f2c7de3bc1b86d06c6be6a159e
Tags	discovery adware persistence ransomware spyware

score

8/10

Table of Contents

Part 1. Analysis Overview

score

8/10

SHA256
bb2aff493d76602afe402f40f810afb329c380f2c7de3bc1b86d06c6be6a159e

Threat Level: Likely malicious

The file WhatsApp Installer (6).exe was found to be: Likely malicious.

Malicious Activity Summary

discovery adware persistence ransomware spyware

- **Boot or Logon Autostart Execution: Active Setup**
- **Loads dropped DLL**
- **Checks computer location settings**
- **Enumerates connected drives**
- **Network Share Discovery**
- **Drops file in Program Files directory**
- **Drops file in Windows directory**
- **Enumerates physical storage devices**
- **Browser Information Discovery**
- **Untrusted Codesign Signers**
- **System Time Discovery**
- **Modifies data under HKEY_USERS**
- **Modifies Internet Explorer settings**
- **Enumerates system info in registry**
- **Suspicious behavior: AddClipboardFormatListener**
- **Modifies registry class**
- **Suspicious use of SetWindowsHookEx**
- **Uses Volume Shadow Copy WMI provider**
- **Suspicious use of FindShellTrayWindow**
- **Suspicious behavior: EnumeratesProcesses**
- **Suspicious use of AdjustPrivilegeToken**
- **Suspicious use of SendNotifyMessage**
- **Suspicious use of WriteProcessMemory**

> **Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary**

> **Uses Volume Shadow Copy service COM API**

> **Uses Task Scheduler COM API**

> **Checks SCSI registry key(s)**

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Reconnaissance TA0043			
Resource Development TA0042			
Initial Access TA0001			
Execution TA0002			
Persistence TA0003	Boot or Logon Autostart E… T1547		
	Active Setup T1547.014		
Privilege Escalation TA0004	Boot or Logon Autostart E… T1547		
	Active Setup T1547.014		
Defense Evasion TA0005	Modify Registry T1112		
Credential Access TA0006			
Discovery TA0007	Browser Information Disco… T1217	Network Share Discovery T1135	Peripheral Device Discovery T1120
	Query Registry T1012	System Information Disco… T1082	System Time Discovery T1124
Lateral Movement TA0008			
Collection TA0009			
Command and Control TA0011			
Exfiltration TA0010			
Impact TA0040			

Part 3. Analysis: static1

3. 1. Detonation Overview

Target	Reported
WhatsApp Installer (6).exe	2026-03-03 17:30

3. 2. Signatures

> **Untrusted Codesign Signers**
>
Description	Indicator	Process	Target
N/A	N/A	N/A	N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Target	SHA256	Filesize
WhatsApp Installer (6).exe	bb2aff493d76602afe402f40f810afb329c380f2c7de3bc1b86d06c6be6a159e	1.1MB

Submitted	Reported	Platform	Max time kernel	Max time network
2026-03-03 17:30	2026-03-03 17:45	win10v2004-20260130-en	898s	718s

4. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe"
```

4. 3. Signatures

Checks computer location settings

Description	Indicator	Process	Target
Key value queried	\REGISTRY\USER\S-1-5-21-1609746302-1884177235-1125644204-1000\Control Panel\International\Geo\Nation	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe	N/A

Loads dropped DLL

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe	N/A

Network Share Discovery

discovery

Drops file in Program Files directory

Description	Indicator	Process	Target
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-lv.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-sl.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-cy.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1948221499\crl-set	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-as.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-la.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-lt.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Sigma\Other	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1948221499\manifest.json	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-be.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-sv.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1354264753\LICENSE	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_2061578646_metadata\verified_contents.json	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Mu\TransparentAdvertisers	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A

Description	Indicator	Process	Target
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-cu.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-da.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-fr.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-gu.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-kn.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-pa.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\manifest.json	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_532535995\manifest.json	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-et.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-es.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\manifest.fingerprint	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_908673474\Filtering Rules-AA	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_908673474\manifest.fingerprint	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_497857687\test.txt	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Mu\Fingerprinting	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_105176714\kp_pinslist.pb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_908673474\Part-ZH	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_497857687\model.markov	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-en-gb.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-hy.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-sk.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_532535995\manifest.fingerprint	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_105176714\manifest.fingerprint	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Mu\Advertising	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Sigma\Cryptomining	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-mr.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-mul-ethi.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-nl.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_2061578646\manifest.fingerprint	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Mu\Social	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-tk.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_186832722\manifest.json	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_497857687\male_names.txt	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A

Description	Indicator	Process	Target
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-mn-cyrl.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-uk.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Mu\CompatExceptions	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Mu\Cryptomining	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-ml.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-und-ethi.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_908673474\LICENSE	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_2061578646\manifest.json	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Sigma\Analytics	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-ta.hyb	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_497857687\passwords.txt	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_497857687\us_tv_and_film.txt	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_908673474\manifest.json	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_908673474\Part-ES	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_908673474\Part-IT	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_400991360\manifest.json	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
File created	C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Sigma\Staging	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A

Enumerates system info in registry

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemManufacturer	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
Key opened	\REGISTRY\MACHINE\Hardware\Description\System\BIOS	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemManufacturer	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A

Modifies data under HKEY_USERS

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-19\SOFTWARE\Microsoft\Cryptography\TPM\Telemetry\TraceTimeLast = "134170327809574376"	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A

Suspicious behavior: EnumeratesProcesses

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A

Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	N/A

Suspicious use of AdjustPrivilegeToken

Description	Indicator	Process	Target
Token: SeDebugPrivilege	N/A	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe	N/A
Token: SeManageVolumePrivilege	N/A	C:\Windows\System32\svchost.exe	N/A

Suspicious use of FindShellTrayWindow

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A

Suspicious use of SendNotifyMessage

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A
N/A	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 4500 wrote to memory of 4152	N/A	C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 4116	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 4180	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 4180	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 4180	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 4396	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 2996	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 2996	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 5992	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 5992	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

Description	Indicator	Process	Target
PID 4152 wrote to memory of 5992	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 3856	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 3856	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 3132	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 3132	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 2616	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 2616	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 1208	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 4944	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 4944	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 5668	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 5668	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 2980	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 2980	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 4176	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 4176	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 1524	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 1524	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 6108	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 6108	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 1784	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 1784	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe
PID 4152 wrote to memory of 1616	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

Description	Indicator	Process	Target
PID 4152 wrote to memory of 1616	N/A	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe	C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

4. 4. Processes

C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe

```
"C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe"
```

C:\Windows\system32\rundll32.exe

```
"C:\Windows\system32\rundll32.exe" "C:\Windows\SYSTEM32\EDGEHTML.dll",#141 Microsoft.VCLibs.140.00_8wekyb3d8bbwe
```

C:\Windows\System32\svchost.exe

```
C:\Windows\System32\svchost.exe -k UnistackSvcGroup
```

C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe

```
"C:\Program Files\WindowsApps\5319275A.WhatsAppDesktop_2.2606.102.0_x64__cv1g1gvanyjgm\WhatsApp.Root.exe"
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --embedded-browser-webview=1 --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --noerrdialogs --edge-webview-disable-crash-reporting=1 --embedded-browser-webview-enable-extension --mojo-named-platform-channel-pipe=4500.5232.4791979270314896356
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=crashpad-handler --user-data-dir=C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Crashpad --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=132.0.6834.160 "--annotation=exe=C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --annotation=plat=Win64 "--annotation=prod=Edge WebView2" --annotation=ver=132.0.2957.140 --initial-client-data=0x164,0x168,0x16c,0x140,0xf4,0x7ffabdb7b078,0x7ffabdb7b084,0x7ffabdb7b090
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=gpu-process --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --gpu-preferences=UAAAAAAAAADgAAAEAAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAAAA --always-read-main-dll --field-trial-handle=1736,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=1720 /prefetch:2
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=1368,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=2064 /prefetch:3
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=2388,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=2368 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=renderer --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=5 --js-flags="--harmony-weak-refs-with-cleanup-some --expose-gc --ms-user-locale=" --always-read-main-dll --field-trial-handle=3704,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=3712 /prefetch:1
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=4496,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4504 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=4512,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4612 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=4212,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=316 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=gpu-process --disable-gpu-sandbox --use-gl=disabled --gpu-vendor-id=5140 --gpu-device-id=140 --gpu-sub-system-id=0 --gpu-revision=0 --gpu-driver-version=10.0.19041.546 --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --gpu-preferences=UAAAAAAAAADoAAAEAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAABCAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAIAAAAAAAAAAgAAAAAAAA --always-read-main-dll --field-trial-handle=3908,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4604 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=3984,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4196 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=4184,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4604 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=3932,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4520 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=3956,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4592 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=4556,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4592 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=4520,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4392 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=2204,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=964 /prefetch:8
```

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe

```
"C:\Program Files (x86)\Microsoft\EdgeWebView\Application\132.0.2957.140\msedgewebview2.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --noerrdialogs --user-data-dir="C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView" --webview-exe-name=WhatsApp.Root.exe --webview-exe-version=1.0.0 --embedded-browser-webview=1 --always-read-main-dll --field-trial-handle=4676,i,1110865089032116611,3096408839280978764,262144 --variations-seed-version --mojo-platform-channel-handle=4388 /prefetch:8
```

4. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	storeedge.microsoft.com	udp
GB	104.83.3.113:443	storeedge.microsoft.com	tcp
US	8.8.8.8:53	store-images.microsoft.com	udp
GB	2.19.14.44:443	store-images.microsoft.com	tcp
US	8.8.8.8:53	c.pki.goog	udp
GB	142.251.29.94:80	c.pki.goog	tcp
US	8.8.8.8:53	crashlogs.whatsapp.net	udp
GB	163.70.151.60:443	crashlogs.whatsapp.net	tcp
US	8.8.8.8:53	dns.google	udp
US	8.8.8.8:53	dns.google	udp
US	8.8.8.8:53	dns.google	udp
US	8.8.8.8:53	dns.google	udp
US	8.8.8.8:53	dns.google	udp
US	8.8.8.8:53	dns.google	udp
US	8.8.4.4:443	dns.google	tcp
US	8.8.8.8:443	dns.google	tcp
US	8.8.4.4:443	dns.google	tcp
GB	163.70.151.60:443	crashlogs.whatsapp.net	tcp
US	8.8.4.4:443	dns.google	udp
US	150.171.27.11:443		tcp
US	8.8.8.8:53	msedge.b.tlu.dl.delivery.mp.microsoft.com	udp
GB	90.244.159.107:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
US	8.8.8.8:53	msedge.b.tlu.dl.delivery.mp.microsoft.com	udp
US	150.171.27.11:443		tcp
US	8.8.4.4:443	dns.google	tcp
US	8.8.8.8:53	crashlogs.whatsapp.net	udp
GB	163.70.151.60:443	crashlogs.whatsapp.net	tcp
GB	90.244.159.107:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
US	8.8.8.8:53	msedge.b.tlu.dl.delivery.mp.microsoft.com	udp
US	8.8.8.8:53	msedge.b.tlu.dl.delivery.mp.microsoft.com	udp
US	8.8.8.8:53	msedge.b.tlu.dl.delivery.mp.microsoft.com	udp
US	8.8.8.8:53	msedge.b.tlu.dl.delivery.mp.microsoft.com	udp
US	8.8.8.8:53	msedge.b.tlu.dl.delivery.mp.microsoft.com	udp
US	150.171.28.11:443		tcp
US	8.8.8.8:53	msedge.b.tlu.dl.delivery.mp.microsoft.com	udp
US	8.8.8.8:53	dns.google	udp
US	8.8.8.8:53	dns.google	udp
US	8.8.8.8:443	dns.google	tcp
US	8.8.8.8:53	msedge.b.tlu.dl.delivery.mp.microsoft.com	udp

4. 6. Files

memory/4424-0-0x0000017BF2EB0000-0x0000017BF2FC2000-memory.dmp

memory/4424-1-0x0000017BF56D0000-0x0000017BF56E0000-memory.dmp

memory/4424-2-0x0000017BF4D50000-0x0000017BF4D5A000-memory.dmp

memory/4424-3-0x0000017BF5610000-0x0000017BF56CA000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\Tmp1BEF.tmp

MD5	a10f31fa140f2608ff150125f3687920
SHA1	ec411cc7005aaa8e3775cf105fcd4e1239f8ed4b
SHA256	28c871238311d40287c51dc09aee6510cac5306329981777071600b1112286c6
SHA512	cf915fb34cd5ecfbd6b25171d6e0d3d09af2597edf29f9f24fa474685d4c5ec9bc742ade9f29abac457dd645ee955b1914a635c90af77c519d2ada895e7ecf12

memory/4424-16-0x0000017BF54D0000-0x0000017BF54E2000-memory.dmp

memory/4424-17-0x0000017BF5A40000-0x0000017BF5A7C000-memory.dmp

memory/4424-18-0x0000017BF5A00000-0x0000017BF5A26000-memory.dmp

memory/4424-19-0x0000017BF56D0000-0x0000017BF56E0000-memory.dmp

memory/4424-20-0x0000017BF63D0000-0x0000017BF63D8000-memory.dmp

memory/4424-21-0x0000017BF9540000-0x0000017BF9578000-memory.dmp

memory/4424-22-0x0000017BF8740000-0x0000017BF874E000-memory.dmp

memory/4424-26-0x0000017BF98E0000-0x0000017BF9A66000-memory.dmp

memory/4424-27-0x0000017BF9580000-0x0000017BF9588000-memory.dmp

memory/4424-28-0x0000017BF56D0000-0x0000017BF56E0000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\Microsoft.Services.Store.winmd

MD5	4aae69886cd900c373d69194dc4241a0
SHA1	50cc74acbfedea48f1225181682253002bced6da
SHA256	44f3a05334de6ca0b43ebd17f6c7f1935630e026f049f28828566e364b7f41aa
SHA512	02289cb11b4090028c5a2fecc69be1ddb8ed0b57125c3c7d898b9937b46da53dcfd3cd7c601c8f7e124f5587ff0a3f4450fa7da0add5abab4ff3903ab23f82c8

memory/4424-33-0x0000017BF56D0000-0x0000017BF56E0000-memory.dmp

memory/4424-34-0x0000017BF56D0000-0x0000017BF56E0000-memory.dmp

memory/4424-35-0x0000017BF3350000-0x0000017BF335C000-memory.dmp

memory/4424-37-0x0000017BF56D0000-0x0000017BF56E0000-memory.dmp

memory/4424-36-0x0000017BF56E0000-0x0000017BF57F5000-memory.dmp

memory/4424-38-0x0000017BF56D0000-0x0000017BF56E0000-memory.dmp

memory/4424-39-0x0000017BF56D0000-0x0000017BF56E0000-memory.dmp

memory/4424-40-0x0000017BF56D0000-0x0000017BF56E0000-memory.dmp

memory/5428-49-0x000001DC55A50000-0x000001DC55B65000-memory.dmp

memory/5448-66-0x000001C410B60000-0x000001C410B70000-memory.dmp

memory/5448-50-0x000001C410A60000-0x000001C410A70000-memory.dmp

memory/5448-82-0x000001C421160000-0x000001C421161000-memory.dmp

memory/5448-84-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-86-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-87-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-89-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-91-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-92-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-90-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-88-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-85-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-83-0x000001C421180000-0x000001C421181000-memory.dmp

memory/5448-93-0x000001C420DA0000-0x000001C420DA1000-memory.dmp

memory/5448-102-0x000001C420CD0000-0x000001C420CD1000-memory.dmp

memory/5448-99-0x000001C420D90000-0x000001C420D91000-memory.dmp

memory/5448-118-0x000001C420FF0000-0x000001C420FF1000-memory.dmp

memory/5448-117-0x000001C420EE0000-0x000001C420EE1000-memory.dmp

memory/5448-116-0x000001C420EE0000-0x000001C420EE1000-memory.dmp

memory/5448-114-0x000001C420ED0000-0x000001C420ED1000-memory.dmp

memory/5448-96-0x000001C420DA0000-0x000001C420DA1000-memory.dmp

memory/5448-94-0x000001C420D90000-0x000001C420D91000-memory.dmp

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Crashpad\throttle_s

MD5	9e4e94633b73f4a7680240a0ffd6cd2c
SHA1	e68e02453ce22736169a56fdb59043d33668368f
SHA256	41c91a9c93d76295746a149dce7ebb3b9ee2cb551d84365fff108e59a61cc304
SHA512	193011a756b2368956c71a9a3ae8bc9537d99f52218f124b2e64545eeb5227861d372639052b74d0dd956cb33ca72a9107e069f1ef332b9645044849d14af337

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Crashpad\settings.

MD5	2aad6b00386718e529da19cbd150b6f2
SHA1	8651958e3c7697d0e3f2a74c89bff71e8d138ed9
SHA256	48aab0d01861c35f96001c2aed4c7a8c00970f974a759fbbcf499db392319c55
SHA512	fa72d61f802167509d854dd74f74663907f906fbb3dbe5282489817af57f75e1f4ffaafcb2f3d3c649d19aeda871dae7014859b4620fe6c38b53171240436c43

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Local State

MD5	569a39cec83f9a67fbcfaf7367cf2fb3
SHA1	78f282a4535636f5e9fbb64a239f4dc2b4341d29
SHA256	e0112bf58d99684bd73fc68495f7f9b2ff32acacad025ea595abb39d10e366a3
SHA512	6a80eefaf623d6b545f6e57f2aa1e7816976dc1d5839ec44af07cfa44bd2a7ede91f4671e9348c3a654f199f2bc6090ded4e46c78364a062e814488018926ccd

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Local State~RFe590b22.TMP

MD5	94c41621a5dd4c3bc8ec1b905f9d8060
SHA1	dc55c05ea448d58ab3330fc2e9037f76ed7f867c
SHA256	fdecd9cb74866c7705269d49df1eff5c8ea1b1a19aadfad4b0dee07e9f68c611
SHA512	e77bd4cc044b9d50882c168459897fad62c9bc4ca7960097b35d37f45dd98fd01c0ac2b88b20cf62c1046d79951ae9e46a88264ac9017145374f474dca821d5b

memory/4180-149-0x00007FFAEB760000-0x00007FFAEB761000-memory.dmp

\??\pipe\crashpad_4152_QOFUDCNEVIHFABHP

MD5	d41d8cd98f00b204e9800998ecf8427e
SHA1	da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA512	cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\Site Characteristics Database\CURRENT

MD5	46295cac801e5d4857d09837238a6394
SHA1	44e0fa1b517dbf802b18faf0785eeea6ac51594b
SHA256	0f1bad70c7bd1e0a69562853ec529355462fcd0423263a3d39d6d0d70b780443
SHA512	8969402593f927350e2ceb4b5bc2a277f3754697c1961e3d6237da322257fbab42909e1a742e22223447f3a4805f8d8ef525432a7c3515a549e984d3eff72b23

memory/2996-172-0x00007FFAE9DE0000-0x00007FFAE9DE1000-memory.dmp

memory/2996-171-0x00007FFAE9DA0000-0x00007FFAE9DA1000-memory.dmp

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\Extension Rules\MANIFEST-000001

MD5	5af87dfd673ba2115e2fcf5cfdb727ab
SHA1	d5b5bbf396dc291274584ef71f444f420b6056f1
SHA256	f9d31b278e215eb0d0e9cd709edfa037e828f36214ab7906f612160fead4b2b4
SHA512	de34583a7dbafe4dd0dc0601e8f6906b9bc6a00c56c9323561204f77abbc0dc9007c480ffe4092ff2f194d54616caf50aecbd4a1e9583cae0c76ad6dd7c2375b

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Local State

MD5	0c5fe4bf99d3ed89d7df19f90e097dd7
SHA1	02646df8a4634c68d5190c1928e56dc40c1dbbcb
SHA256	06e503a2b5fbda34c5b445a8ed46e0885ffa7b49deb296e10ddfa068fad85e3f
SHA512	6bff6ba45236117d341bbef9fb94cd27b277b57432b199664305e91c177bd8017ac6b65b567746ccd298d934ce3c5497b31cb6803f4b4c2549dfc54baaf772fd

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Local State

MD5	856d9272cbcf3111fc6672cc7762cbf1
SHA1	b15104b3390700d8ae327015112a11a95d45c843
SHA256	2c7ab94cc4dbe54f9b0891ed31febe0a62e216e6301e2a2d9188c379ca461c41
SHA512	318c3fc35287d4dbc632557d1bde0f4bea34c8420346a7aa3a277653678060f0df760e794c4278dc404e17bcd2b6026eb8d885abc7afa14a841b4e51fc9ec29b

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\Network\15 84d1-4aa1-b518-24a67e66ee43.tmp

MD5	d751713988987e9331980363e24189ce
SHA1	97d170e1550eee4afc0af065b78cda302a97674c
SHA256	4f53cda18c2baa0c0354bb5f9a3ecbe5ed12ab4d8e11ba873c2f11161202b945
SHA512	b25b294cb4deb69ea00a4c3cf3113904801b6015e5956bd019a8570b1fe1d6040e944ef3cdee16d0a46503ca6e659a25f21cf9ceddc13f352a3c98138c15d6af

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Crashpad\settings.

MD5	85942bf53cb8cc9737b115fe1af94b58
SHA1	70b32d6cb7445e7151c8ae0712440d212653ef6e
SHA256	f1eced243eb25e2e0363a87bb1621fff666fbf6afe8ea1e10b858f2476bb2b8c
SHA512	fc3ce17faca74184045281f2f0d4e41cd273916b5d31ecd2a6c99322d55e5bc9674e3213fcac0f22b79b495be0bfa97ce2b8c69bcd877dfc4b7609e12cce55dc

memory/5992-270-0x00007FFAEB760000-0x00007FFAEB761000-memory.dmp

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\DawnWebG

MD5	41876349cb12d6db992f1309f22df3f0
SHA1	5cf26b3420fc0302cd0a71e8d029739b8765be27
SHA256	e09f42c398d688dce168570291f1f92d079987deda3099a34adb9e8c0522b30c
SHA512	e9a4fc1f7cb6ae2901f8e02354a92c4aaa7a53c640dcf692db42a27a5acc2a3bfb25a0de0eb08ab53983132016e7d43132ea4292e439bb636aafd53fb6ef907e

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\DawnWebG

MD5	0962291d6d367570bee5454721c17e11
SHA1	59d10a893ef321a706a9255176761366115bedcb
SHA256	ec1702806f4cc7c42a82fc2b38e89835fde7c64bb32060e0823c9077ca92efb7
SHA512	f555e961b69e09628eaf9c61f465871e6984cd4d31014f954bb747351dad9cea6d17c1db4bca2c1eb7f187cb5f3c0518748c339c8b43bbd1dbd94aeaa16f58ed

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\DawnWebG

MD5	d0d388f3865d0523e451d6ba0be34cc4
SHA1	8571c6a52aacc2747c048e3419e5657b74612995
SHA256	902f30c1fb0597d0734bc34b979ec5d131f8f39a4b71b338083821216ec8d61b
SHA512	376011d00de659eb6082a74e862cfac97a9bb508e0b740761505142e2d24ec1c30aa61efbc1c0dd08ff0f34734444de7f77dd90a6ca42b48a4c7fad5f0bddd17

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\DawnWebG

MD5	cf89d16bb9107c631daabf0c0ee58efb
SHA1	3ae5d3a7cf1f94a56e42f9a58d90a0b9616ae74b
SHA256	d6a5fe39cd672781b256e0e3102f7022635f1d4bb7cfcc90a80fffe4d0f3877e
SHA512	8cb5b059c8105eb91e74a7d5952437aaa1ada89763c5843e7b0f1b93d9ebe15ed40f287c652229291fac02d712cf7ff5ececef276ba0d7ddc35558a3ec3f77b0

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\ZoomExtension\manifest.json

MD5	5378fe112c90293fb4eef99e1702b19a
SHA1	fb46d7e68dd0ae10485c5492f0b08b54d3856322
SHA256	0a36950b6a3b4d2f2fd1188877b8c92192c549976c5226b910ff60d6d0ae6f7c
SHA512	98f5846e5ea14b09f56931058d09ead41d89650bc43fd3a4b715bb2c9c2ccec876acb77202148b5b126bc3d06548c4ddd0e15e3e8f727c1da960c7cc1c5a7f4e

memory/4424-464-0x0000017BF3350000-0x0000017BF335C000-memory.dmp

memory/4424-465-0x0000017BF56E0000-0x0000017BF57F5000-memory.dmp

memory/5448-469-0x000001C421130000-0x000001C42113C000-memory.dmp

memory/4500-470-0x0000027458E50000-0x0000027458F65000-memory.dmp

memory/4152-473-0x000001F5111A0000-0x000001F5111AC000-memory.dmp

memory/4152-471-0x000001F5132A0000-0x000001F5133B5000-memory.dmp

memory/4152-472-0x000001F511160000-0x000001F51118C000-memory.dmp

memory/4116-474-0x00000243ECEA0000-0x00000243ECFB5000-memory.dmp

memory/4180-475-0x0000021141A00000-0x0000021141B15000-memory.dmp

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Local State

MD5	4aef733dacc4c3d04a3a70e94a673000
SHA1	da587a65d3b4f902611127194ba6d3dc9e5148db
SHA256	bba5950917ef6b1cca7bf7a73b2068d95e6065a70272d21092087ac831924a34
SHA512	6c38ee290eeff795ca61081b275dc0ef3959bcaf017baca5f6fd6f78da9bd7b34036ecc9d5324aa7b2d57823c24476e117590eaaf9c2a0509aacfafade5b172a

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\Preferences

MD5	cca34842cfb4ebbe7cf152a2d2c49045
SHA1	69515329f8091a666a6f4ff174c90d74a137024a
SHA256	ba15b18c27b5e205797e0070e10c7be4630e4c92187e84181715c7cb0af9e09c
SHA512	c319cd63893fd62676be312a3dbcff07ed59231e2b0d24cc34239bbf4a4e4e35b88cec606ae6a19e4857c652112b5a11484e096290ccb0af32ef59b95ffc3c1a

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Local State

MD5	10a09ef3936a6d2ed5062ed394e4d4b3
SHA1	1a1d360963f9a6048567ee31830163d3fa839dc2
SHA256	038603e4d30e07bad90914ee5917110843488d2dcc140c628df604fe724fd8dd
SHA512	a99dee78795af11db660a5f586c8c96955f7d990796e716e8f2017779b92476ee902aee2405d3a955322d0383782f5e118cdbff2cc453985ae2839bfc8e19d21

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\Preferences

MD5	b1c84b49d21aff5f66d1c1634fc42c21
SHA1	7db9e9da8a911aad3a86657942e966a280cad936
SHA256	4ea3b36537f5fcc2c1e90a0a2120d856a73e884dac39a5d52e127b3ab0c83687
SHA512	6a7441d20f08e882d2c817cb9d1cd7eba77b3c4db2445f9aac6947ea5632a6dcbc832b060269eef90189db3277aea3bff8aaed2863d8a59626e7eb6ed559960e

memory/4152-564-0x000001F513F00000-0x000001F513F27000-memory.dmp

memory/4152-565-0x000001F513F30000-0x000001F513F6B000-memory.dmp

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Local State

MD5	987c4631b83686fdc9f2a36095daa791
SHA1	2138e0ac3332ce95024b2b20fcb5da4f9061fd6b
SHA256	84f025481933630f038a7e0cfef77d8508bcebff1d23271e5ce341b0af823b61
SHA512	9d1fab75c508e3dad37d4f649cd3e60b05dcca9d67cd82f9ee8ce0d48f1ad4ba6196ef6b84642d73640a0ce690733b2f2d0db857294c61b779c19328cb3fc066

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Default\Preferences

MD5	19f076375a3ebd599cce778987c51202
SHA1	74a2fde31bffe048e58f295bdeaa96adc4997a9e
SHA256	7912eda615925dbb741b6563dad4ccb44175f4045a7520d2659de4fd8a2a114b
SHA512	7157d47e4670b00295e9d94dd993b77e8cec4ff377bf9408dd2787837502c7942b6d0213d42ddf898fa70ef6335da15b021bf5494171668eff8669b65089ab99

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\AutoLaunchProtoc

MD5	1de85fec2dfcc28011a7c2aaab95eb5f
SHA1	80e8c954bfbe8f7ee5a2335c8d969ae033935dc3
SHA256	4fd800e7b1a5fb24b13fac2e31946d205012b7c28d8c61580b0669b2fa3517cc
SHA512	9c7dd37eb0c094b6aa05201e7c71a8f33b9db81284223bcfa595a44a6ac95d5a6820ab6f07b7aa8d26bf207454e94277bf35332e9c009ee63f083752b6b51750

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_186832722\manifest.json

MD5	fbebd68ecaa98928909421f66909c054
SHA1	99d787d90f7ed2e5ad924f9c5668eb988b5a6c07
SHA256	ba5c9096d20a482aaa1aa9e5f98ad6127d3e97c2f21de84f7c78d9b8073c8e26
SHA512	749a3b2be47fe28399dc763888654a3e8d397e06e8d3c3af3965bb45846a1336e6ab4ca82c82c3df846b34a2afafa2156f2690e9bf347ab175408dc0171c61cc

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_186832722\manifest.fingerprint

MD5	c28ffa45708f10e3a35143ed2708782f
SHA1	84a03f2615333c9311dbf79d6f58f56b5c009163
SHA256	c236a2ac7741d48e1c56980652331cb3f1f12baf937baf0b280600fbafb143e3
SHA512	beac0eacff45a152eb2a50f4d72db2933b8f8ba97e6f0a9f6811abe866fef5c7c83068151915dbdffaccaee5d0cd335d182671f44dbab6da2222266ff8a28ff0

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1948221499\manifest.json

MD5	7ef3c71464d0fef472bc1d81fd363c62
SHA1	230e8ec0f849bf34d444c55ef548ba0c9c94d39b
SHA256	98821f71a1973ac61b45967ce0c121eb598ac6e95abaa23c912d2f33e4237d8c
SHA512	f74b96ec3b9569e360a02bfdd4fe237efad8ee2a5deaf46db891bcadd39dba22fd6d59a4e9aafe5511152625ce9f468519dadd53fc0c9b6c8826dc58cbe6cd7c

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\CertificateRevocati set

MD5	d01869348d5a783f61f90cbb27b82a78
SHA1	d4eccc91435adaf01f8589cf7f3589cf65425de2
SHA256	6ddcaf50aaff98b960d067054ce2ce17872ac0719d02abbb7fe56b9eabc818f2
SHA512	7ad7f27d1f559d1f50f1f009518ccca5d6d01696cd70657ad94c9fe37db7bbe06e4afc13170bc5c065cf72d69a92c3df78f637b7faa2f968bb89aa154fe371da

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-as.hyb

MD5	8961fdd3db036dd43002659a4e4a7365
SHA1	7b2fa321d50d5417e6c8d48145e86d15b7ff8321
SHA256	c2784e33158a807135850f7125a7eaabe472b3cfc7afb82c74f02da69ea250fe
SHA512	531ecec11d296a1ab3faeb2c7ac619da9d80c1054a2ccee8a5a0cd996346fea2a2fee159ac5a8d79b46a764a2aa8e542d6a79d86b3d7dda461e41b19c9bebe92

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-hi.hyb

MD5	0807cf29fc4c5d7d87c1689eb2e0baaa
SHA1	d0914fb069469d47a36d339ca70164253fccf022
SHA256	f4df224d459fd111698dd5a13613c5bbf0ed11f04278d60230d028010eac0c42
SHA512	5324fd47c94f5804bfa1aa6df952949915896a3fc77dccaed0eeffeafe995ce087faef035aecea6b4c864a16ad32de00055f55260af974f2c41afff14dce00f3

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\hyph-nb.hyb

MD5	677edd1a17d50f0bd11783f58725d0e7
SHA1	98fedc5862c78f3b03daed1ff9efbe5e31c205ee
SHA256	c2771fbb1bfff7db5e267dc7a4505a9675c6b98cfe7a8f7ae5686d7a5a2b3dd0
SHA512	c368f6687fa8a2ef110fcb2b65df13f6a67feac7106014bd9ea9315f16e4d7f5cbc8b4a67ba2169c6909d49642d88ae2a0a9cd3f1eb889af326f29b379cfd3ff

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1005342061\manifest.json

MD5	2617c38bed67a4190fc499142b6f2867
SHA1	a37f0251cd6be0a6983d9a04193b773f86d31da1
SHA256	d571ef33b0e707571f10bb37b99a607d6f43afe33f53d15b4395b16ef3fda665
SHA512	b08053050692765f172142bad7afbcd038235275c923f3cd089d556251482b1081e53c4ad7367a1fb11ca927f2ad183dc63d31ccfbf85b0160cf76a31343a6d0

memory/1208-904-0x000001A030980000-0x000001A030981000-memory.dmp

memory/1208-903-0x000001A030980000-0x000001A030981000-memory.dmp

memory/1208-905-0x000001A030980000-0x000001A030981000-memory.dmp

memory/1208-909-0x000001A030980000-0x000001A030981000-memory.dmp

memory/1208-913-0x000001A030980000-0x000001A030981000-memory.dmp

memory/1208-915-0x000001A030980000-0x000001A030981000-memory.dmp

memory/1208-914-0x000001A030980000-0x000001A030981000-memory.dmp

memory/1208-910-0x000001A030980000-0x000001A030981000-memory.dmp

memory/1208-912-0x000001A030980000-0x000001A030981000-memory.dmp

memory/1208-911-0x000001A030980000-0x000001A030981000-memory.dmp

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_532535995\manifest.json

MD5	af3a9104ca46f35bb5f6123d89c25966
SHA1	1ffb1b0aa9f44bdbc57bdf4b98d26d3be0207ee8
SHA256	81bd82ac27612a58be30a72dd8956b13f883e32ffb54a58076bd6a42b8afaeea
SHA512	6a7a543fa2d1ead3574b4897d2fc714bb218c60a04a70a7e92ecfd2ea59d67028f91b6a2094313f606560087336c619093f1d38d66a3c63a1d1d235ca03d36d1

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_908673474\manifest.json

MD5	6658e8d6901ebdb2b695444e181b6348
SHA1	34c4bce8c106ad7c8ba03d56f702b868a9ae67ed
SHA256	a1774d7a0ac3f90fe6fbed83045377b838af48811380d5ad88809222168c22eb
SHA512	615aa2777141a88f0d0904e7c73de3affadab0e7bff76fd11b98c8970f9b44fff5186bd4ca721c8960f1b57b4e35323826d52d5fc09d10a25b21b4ab46167d70

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Subresource Filter\Unindexed Rules\10.34.0.81\LICENSE

MD5	aad9405766b20014ab3beb08b99536de
SHA1	486a379bdfeecdc99ed3f4617f35ae65babe9d47
SHA256	ed0f972d56566a96fb2f128a7b58091dfbf32dc365b975bc9318c9701677f44d
SHA512	bd9bf257306fdaff3f1e3e1fccb1f0d6a3181d436035124bd4953679d1af2cd5b4cc053b0e2ef17745ae44ae919cd8fd9663fbc0cd9ed36607e9b2472c206852

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Subresource Filter\Unindexed Rules\10.34.0.81\Filtering Rules

MD5	43f62d9f35fa6597cec4e2ad5643e282
SHA1	8dba6404724ffd6a2e89901e8dc6e5e55fed3374
SHA256	5e301c48e6d7290990971e9f0bcb2263c8adba06ed0a2c6db5086949825d999b
SHA512	91891d23464f89e6769d9ec7a28867e28f77925e6e3b3b75fb628d8672157ba239676c07699c931ac307a21ccc4dae95dd707d410f988ff82be4015103d4d6a3

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_2061578646\manifest.json

MD5	44791df1f32899ba8f0fd1f235cd4711
SHA1	e5ab30e8b7610e92c81c99adb110e3a429fc3174
SHA256	8f8dae05e2623c591dc44dc5a91385b4355da91492a770f0ca99b509db6533e2
SHA512	729578ec403ba1410c5826f622d4db774d68e243112351f50cb5fcf231ebdf7fd9759bb5e2bd4a7bd6433c147ede44b78f4eef2eb08c456d4a430b55a149edd2

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\TrustTokenKeyCom

MD5	48cb5a96ba70f0dfcca0a2185a9a0c79
SHA1	efdbdf44f7cfea2e3b34c6b2fc0dc37a1b5cef3e
SHA256	722047d2502aaec9c2c80b0f7d3b60b29d3f6aee27d656f489e4fbca9a7c1a00
SHA512	77eb7bc1bdea2b121b8d95fd8b5d14603d5e105dbf8c8e777b44109b1eb2ba65785ee3a094e18ffb591f81fe140ff83af1618d82680a5bb3a29144c58895dd2e

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_400991360\manifest.json

MD5	ba25fcf816a017558d3434583e9746b8
SHA1	be05c87f7adf6b21273a4e94b3592618b6a4a624
SHA256	0d664bc422a696452111b9a48e7da9043c03786c8d5401282cff9d77bcc34b11
SHA512	3763bd77675221e323faa5502023dc677c08911a673db038e4108a2d4d71b1a6c0727a65128898bb5dfab275e399f4b7ed19ca2194a8a286e8f9171b3536546f

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_105176714\manifest.json

MD5	50558b365ad40a8213fb79e84d42ffa3
SHA1	497d5ad94af7cecd6457fbd5723b6635ccd67c6b
SHA256	8ee8a2fb7167ad2dcf2dd6f56074509dedd711b1825dcba2629af48c89eeebbe
SHA512	165a117c8f8247263c3328def089e5bc159895e1d4375bd3df93df8f9208c571dc7e3fb98389fa36952c6f3d8f3add4fe5c97b22bddc01ef7c4ac37477cc608a

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\PKIMetadata\28.0.0

MD5	3ef7a7be0ecfef355a5d5d6e77ebddfd
SHA1	5c6e47340a710019b97b1fd58624f714420b79f1
SHA256	576d77d3085ff9156298e60dee868364cabab7911edf6f9a4d3ad5f351d5059f
SHA512	812f5a4e1f572b7a012add71bc210281fd362f48ba5a863b2e5a7d7b6405dd08632dc39ce650a0d032f926d1e41acd8f1c84d5b60552ad9ac98ad6d2abb7f265

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\PKIMetadata\28.0.0

MD5	269f13e71015d2f9da1fc0e0e22b27c7
SHA1	67b35f4044517ec8b169d27d354a61e2f095895a
SHA256	1b9ee7a3aec303937fd884335b23591b55e0d5901d1ee25aa25800d1c202a24b
SHA512	039d3f870a4475ded4f972891059a4ebc467588f349d0310e47c9c975c793fbfe4179dc64f5c2616914aa97bcd5e83d6333f5de113f5c56c2fc3f2b7bb012dec

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\PKIMetadata\28.0.0

MD5	b83d9c00b73ffd5b6945370fee4bdb26
SHA1	dc5e7ab71b439abe18cde2c4309ef4452220d0de
SHA256	b42799f862739fed511f2527d4796690e23014ecdc02489074df4c44c60f272d
SHA512	fff0baa29fcb0253be4f916dd6fde7efdf6b20c49c851e4ff6a027b055a7a48a8dbb74827d55b525c3b1e7e53e27f84e2563f8cb5b7092911d651f4cdbb967ba

memory/4500-1267-0x0000027458E50000-0x0000027458F65000-memory.dmp

memory/4152-1268-0x000001F5132A0000-0x000001F5133B5000-memory.dmp

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_497857687\manifest.json

MD5	fb0d9796a86299d3689982f7a949dc6e
SHA1	6179cd612ac0dcc44d0659c7c99d1e0aecbf206e
SHA256	c0622dadf4ec10ce5f4a64e3f24956b750345dcc194d0bd3ff73cfce1bf6081e
SHA512	e3e1a18be661da9d450a30a37d24dc08dc8de628a104ce0f4197214ce6f27a2bf9de3eca1c1697fcfa3c601787ca7a6b5e30a5fe3d6ae3b2c10f1ab34af22fd0

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\manifest.json

MD5	a4d9ab812da8b2906ff9d46f9ffc07c3
SHA1	48b428dc760bc008058e6df47a9f05f2f86b4abb
SHA256	68683970ce6d7de9a2043c34129106ae68af21a3b0a3c53cb59695640a7c1cbc
SHA512	5a2ba950ed85ee55bc1402d57d09ca8d54c0c2df5b43a402bb8bf3668920a40d584fa18d270376b046e23be00698bd1399ef6a0b695ee6c0b99fb454616b1cb6

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1474032856\Sigma\Staging

MD5	0163de1b14421d4eee3757ff76fd81e4
SHA1	96c75c4fe1e3f33a367f45293bd1bd8bff1c06f4
SHA256	411a706def2e70f96a507208bf80bceb93e950c4c2d671cd1ddb4134ce54b2a9
SHA512	80114d59db8f3654dd6821589e5ad03daa923a35610a372756a8865b3e769621e32ef2aed92c2494de2b9fc06d9796b12f1e3bb75873ed794e8c9ae8a0d5e965

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\manifest.fingerprint

MD5	0f487a41f1bb9a49dfc5814815dc8b1e
SHA1	39e5af8034fab47bdfbaa2a66455c74185756f0a
SHA256	f96cf59ef5cdf10cdebb367e16c6736d188af934062a8721eb9d60539556a2a9
SHA512	bbbd1619eead82c70cdc0f72867db2ffdd4a45cb908c81e852eec8c1293bcafb90c554bc3d51afab7fd7e478efc15aa9ad90fe1b56a01d0012ecee493184d36a

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\CompatExceptions

MD5	108de320dc5348d3b6af1f06a4374407
SHA1	90aa226d3c9d50cf4435ecdd2b8b0086d8edeb8b
SHA256	5b462316a51c918d0bae95959bf827cb9c72bbd84ffb0e43b750aa91fbf3ba53
SHA512	70f30c45e20b7cddd0cba6476af9338975cec8e40b8b19603af5fa859a34c6eb2138957daaa263633fe65213e2186402d05d9d29ad53e8f311335555116314c2

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Sigma\Entities

MD5	751e7cc660220e7464935a9b90643274
SHA1	05a725af45c74a9e129839b2fa7acca5d83066d8
SHA256	0f305323c627cf0c790831c7e0bc38455b7a99983c4ab5bd9d2d9567766c3499
SHA512	bc879a9bed224b6abdaed2581f948fcad53361b17dc76d5b5df10607ac893db2f39bc5ce5fbbe86e6392ae66f29fc93ac1079fd2d029b9338697b004325c4b36

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\Entities

MD5	478a605d5578236f2d1ddc93c2f22456
SHA1	917f05453d497b3e3de684a905e141972c34a267
SHA256	f6e93c83d9e3cfdff064535647cee76fc85aa1c86fd22a93dcf3d2c377346d94
SHA512	26d75309976fac0bd03ffe7596209c50ead7518584dd9f27d12a86d80ecec0889bb58da1b8dc8cdb38fc6bfdca7928a54c5a15903c4b8d293633d4d58ec147b5

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Sigma\Other

MD5	7bb2f4076e4f47781b77d811b21ef1ff
SHA1	fc0feddf6f52841bbd780d21b8e0ddff74fd70ac
SHA256	c9ab8dbc87043c71dd649fc06bb006e7f62e81c973c37b125afb88e654e436f8
SHA512	28356614bc38576ecb37218f9f6f631bd9e55573206c3aa854b91956a33fc828c71f42c7dc7dc6aa86540dab8e345b8f88bf9c6eb56e49824f492854c193b27b

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Sigma\Social

MD5	fbfc314bba2160b09a3376521c762772
SHA1	3566357486c5d466958334e813c90c0a97bfc985
SHA256	e520603e6fb543cd078b2a7dbd8ccfc175e9aecf71654fc19785927a014d3435
SHA512	e4383491ce5170d0daf4abee61484c62611dfc604549b537d0080f24bfb8cf379ec3efbfb6caf10e7c066ec06457fb077832d5f780d226f0a957f624e0ba9383

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Sigma\Fingerprinting

MD5	5330ccc991b45c6f2777d23c7d8afe8d
SHA1	d11187c035458fe1201608a91062962903de2e53
SHA256	ec0fcbf71d58e707aaf6ba8d3c0719972f26727febe03f8efbf570b9635faddf
SHA512	2db42b7a6b7f2170f6cad2a26a606ff6357cb8c707ba9947baab14dd7f566df04a274e46e36cee72c43ee87ebf4d455b4af3f6da973f29bdbefeb0304f1d6f93

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Sigma\Cryptomining

MD5	4ec1eda0e8a06238ff5bf88569964d59
SHA1	a2e78944fcac34d89385487ccbbfa4d8f078d612
SHA256	696e930706b5d391eb8778f73b0627ffc2be7f6c9a3e7659170d9d37fc4a97b5
SHA512	c9b1ed7b61f26d94d7f5eded2d42d40f3e4300eee2319fe28e04b25cdb6dd92daf67828bff453bf5fc8d7b6ceb58cab319fc0daac9b0050e27a89efe74d2734e

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Sigma\Content

MD5	dee2a727844dd3cea088941e82722406
SHA1	24ebec9b92eeb6af83841ab02e858f415580f719
SHA256	d99df5936c57a50aebb7f0a3ca65fcc682f523ace93641fbcfb9b09cfb71c739
SHA512	e48edf5f6dcbbd615f42f1b3181b2998bd700508094466009a6a48193a48c3e30e6c4d71cc43aae81d18a88ad9fd7e28eb50a0a52ca6889a270001fecdb64dfb

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\Analytics

MD5	db9a3dbc4820c8d84a0a569be1234dc0
SHA1	78fe9b49b800627cd2eb458cbe0251591a2a693a
SHA256	163a5318312b814104d244a4b37b676a02f827068820aa60fc069e6346cb2b75
SHA512	a6735713a801d28e644b31f34335e29d55a46d4b263e923cbec9b57fd18f8b0cecf9b78fab578065207080faa5e81156d04c8fbedb436b718893b6d17123742c

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Sigma\Analytics

MD5	e018dfa2df54c80ffbfd02c6d2ff5430
SHA1	de3f876b05355c6024d76f1bc24a552e532e2a2a
SHA256	33d2b069ea874c12ec96242ca7eb539c1086d38ac6c2e4858c0efcd74fc632e5
SHA512	b6d7886b4094837b271d1aa1f72b8c52197052752186604bcb83e17f85fa4a22e658628f79eca7d164ace781555abaa07c423a380fe87006aaed77f53e37838

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Sigma\Advertising

MD5	6959a6835772c67f4e72105e4be259a2
SHA1	72d1fe9070a5c0eed55d989cbd961dbc5442796c
SHA256	868f3ed3f86f1e82a5041f0a7b382bdd720e411531df2dc680da34eb60580b75
SHA512	98085236a15e810642602e5dd475aa5a9532bb38917aef784e977bb398b3f9e39f7966370d39c1b554cf3e39858713e8b45bc27fbdb8a701b2a903e453a67591

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\Other

MD5	cd0395742b85e2b669eaec1d5f15b65b
SHA1	43c81d1c62fc7ff94f9364639c9a46a0747d122e
SHA256	2b4a47b82cbe70e34407c7df126a24007aff8b45d5716db384d27cc1f3b30707
SHA512	4df2ce734e2f7bc5f02bb7845ea801b57dcf649565dd94b1b71f578b453ba0a17c61ccee73e7cff8f23cdd6aa37e55be5cb15f4767ff88a9a06de3623604fbf0

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\Social

MD5	1d06d58fe9131c14ba5ba5ff740b020f
SHA1	e6ed812e23e201b20170e928686a5d612165df85
SHA256	4955c3e7f56641a4ae0ce9c79b4ceee4b21733b0f6dedc980bf8d822a792eba2
SHA512	2854c73c6ef4d271d0e992113732ad65e406d6310711551952b4d451e2c577a2c3dcb06052e3ab30003b01619a39e87e5dd28d54f459f94efe879d1a79039b8f

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\Fingerprinting

MD5	3d90e5235a4bee8f1dccfc2aecf7c585
SHA1	5beb333084b3af33e7fbd8c83326e18650a87f85
SHA256	c7d2b05ff6e790af78b0f1f341219fdb554dc5e14fbf3e3981819fccdd1ddfed
SHA512	c81af723cadaa57f638b9dbc60aca5d2600cebb8282d78a7b86edc6b473bd3a1768c8fde1b11d50b6b967b2866495655de095779737780384 34bf4b513ba74a7

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\Cryptomining

MD5	95aa820d67ec466eb3444a9458eb7e56
SHA1	f93e178ff40310e071e4d596f0aff0514666f787
SHA256	1e92781e88ee786bf6d1d5cb71d467a92fe7f281f2d1e548524bf119d7ddc700
SHA512	15281c334f013f0200ca2d6faaaec81dc5602058cf3522b805e21ca5f031cb4ca68606d353e6745bfb86f07fdd6ccc892942aee5ad7cf0f9f0798a4d7f497a47

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\Content

MD5	26c006f350f70dbc8c18098b773c3d4c
SHA1	eb015f7010dd74c874675d0599e634027363b7b4
SHA256	7869993fcb93b302598643be96c6ab94c4f3be47c9fc344959773c754291376e
SHA512	0f56d119a5f89689d0e45a6163133048aa95255447c4156d4fb2565f45c32dbb95adc39666a833d2127ce57f3f4198ce45d2a174955ec088bcdd2f74f59b3f6b

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\Advertising

MD5	3495430eefd1e96e8bd95b67ccab0f91
SHA1	54129d2d72e062ad36a66922331818e81bd34df3
SHA256	5989ccf9a58e4ffd47c2422bd8dfcb3ea4e1d412fbdec2291385a9955af9eace
SHA512	9197537719b70837ce997cd2b168c6bf6fe877811f81459a0c0f1363b7179960594761df147c85034c628b8e9a3463084ac26fb8bcc3fbc765089adfeea56f6b

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Sigma\LICENSE

MD5	5b7baf861a48c045d997992424b5877b
SHA1	2b2bd9a13afe49748abf39faf9eb29ed658f066e
SHA256	44071e0fcffb9a9a32e8fa7010bb18dbc41afd0b176f81bf700b15b638a88a51
SHA512	4820b41aa5ff4d934a583e1f0b93b1512631102bb2dfdb74792a2f0dcf9907da7680c02a5ddd2492a1e6d58cdada3453d9e38bb8deab6ce831ff36a7f8de016c

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\TransparentAdvertisers

MD5	57d5a3548911886de2f3bd3172e808ed
SHA1	ca932af3b25f245ce931fbc6cf10299e5fbe35a7
SHA256	d2cd0bef5f45daf490c53e705d6f67dfe12390c72a00efa6f5117432bd8edb8c
SHA512	933194509d305b2a60b38c149ba1d74e142ef15647242b287844d263006d33ffa38b6ea263c89cb821a9277d41f0cfda95a0eda830f3a5ef8df5ba80d3bbc818

C:\Users\Admin\AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalCache\EBWebView\Trust Protection Lists\1.0.0.34\Mu\LICENSE

MD5	d32239bcb673463ab874e80d47fae504
SHA1	8624bcdae55baeef00cd11d5dfcfa60f68710a02
SHA256	8ceb4b9ee5adedde47b31e975c1d90c73ad27b6b165a1dcd80c7c545eb65b903
SHA512	7633623b66b5e686bb94dd96a7cdb5a7e5ee00e87004fab416a5610d59c62badaf512a2e26e34e2455b7ed6b76690d2cd47464836d7d85d78b51d50f7e933d5c

C:\Program Files\chrome_Unpacker_BeginUnzipping4152_1354264753\manifest.json

MD5	580786a5ec9eb650dde3e0e75db8588a
SHA1	8c0835d1a6bf82e753b624440e9674d649696ead
SHA256	25ac9b79df29fa869b4c9f4ca3bdbc3a85f6122f5a8efab5a1216d577099becc
SHA512	c8d41e16b291157e2afbf978469eae4c017d1ce3b941b93ae710e2bbaaf4c3e601db45e579d22b957b7a1ec48cba788015725a2fa23cf02f2d66010ef4fdd0a0

memory/4500-1805-0x0000027458E50000-0x0000027458F65000-memory.dmp

memory/4152-1806-0x000001F5132A0000-0x000001F5133B5000-memory.dmp

Part 5. Analysis: behavioral2

5. 1. Detonation Overview

Target	SHA256	Filesize
WhatsApp Installer (6).exe	bb2aff493d76602afe402f40f810afb329c380f2c7de3bc1b86d06c6be6a159e	1.1MB

Submitted	Reported	Platform	Max time kernel	Max time network
2026-03-03 17:30	2026-03-03 17:46	win11-20260130-en	899s	895s

5. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe"
```

5. 3. Signatures

Boot or Logon Autostart Execution: Active Setup

persistence

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000\Software\Microsoft\Active Setup\Installed Components	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000\Software\Microsoft\Active Setup\Installed Components	C:\Windows\explorer.exe	N/A

Loads dropped DLL

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Enumerates connected drives

Description	Indicator	Process	Target
File opened (read-only)	\??\F:	C:\Windows\explorer.exe	N/A
File opened (read-only)	\??\D:	C:\Windows\explorer.exe	N/A

Drops file in Windows directory

Description	Indicator	Process	Target
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_132762391\sets.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_808274551\extraction.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_668123467\deny_etld1_domains.list	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1639303045\crl-set	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\TransparentAdvertisers	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Sigma\Entities	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_981733079\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\Entities	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Sigma\Fingerprinting	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_981733079\kp_pinslist.pb	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Description	Indicator	Process	Target
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_668123467\deny_full_domains.list	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1639303045\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1761439032\safety_tips.pb	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1639174249\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\Content	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1946387131\protocols.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1929768173\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1929768173\office_endpoints_list.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_132762391\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_808274551\classification.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_808274551\travel-facilitated-booking-bing.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_649655351\autofill_bypass_cache_forms.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_649655351\edge_autofill_global_block_list.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_649655351\v1FieldTypes.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\Social	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1761439032\typosquatting_list.pb	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\Staging	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_132762391\LICENSE	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_808274551\automation.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_184510105\keys.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\LICENSE	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_132762391_metadata\verified_contents.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_808274551\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_184510105\LICENSE	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Sigma\Cryptomining	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1754071788\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1948944278\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1639174249\data.txt	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\Other	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_14636026\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_184510105_metadata\verified_contents.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_668123467\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\Advertising	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Description	Indicator	Process	Target
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_898879799\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1929768173\smart_switch_list.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_2119453888\domain_actions.dll	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1761439032\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\Fingerprinting	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Sigma\LICENSE	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_649655351\regex_patterns.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\Analytics	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1754071788\nav_config.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Sigma\Analytics	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_981733079\ct_config.pb	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File opened for modification	C:\Windows\SystemTemp	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_808274551\travel-facilitated-booking-kayak.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_668123467\deny_domains.list	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_649655351\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\CompatExceptions	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Sigma\Staging	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_14636026\well_known_domains.dll	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_2119453888\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Mu\Cryptomining	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Browser Information Discovery

discovery

Enumerates physical storage devices

System Time Discovery

discovery

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Checks SCSI registry key(s)

Description	Indicator	Process	Target
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\FriendlyName	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{78c34fc8-104a-4aca-9ea4-524d52996e57}\005A	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{51236583-0c4a-4fe8-b81f-166aec13f510}\007A	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\ConfigFlags	C:\Windows\explorer.exe	N/A

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{cf73bb51-3abf-44a2-85e0-9a3dc7a12132}\0006	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{78c34fc8-104a-4aca-9ea4-524d52996e57}\005A	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\HardwareID	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{51236583-0c4a-4fe8-b81f-166aec13f510}\0064	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0003	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{a45c254e-df1c-4efd-8020-67d146a850e0}\0011	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\0004	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{540b947e-8b40-45bc-a8a2-6a0b894cbda2}\0009	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{cf73bb51-3abf-44a2-85e0-9a3dc7a12132}\0006	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{259abffc-50a7-47ce-af08-68c9a7d73366}\000C	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\0004	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\HardwareID	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{a45c254e-df1c-4efd-8020-67d146a850e0}\0011	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{b725f130-47ef-101a-a5f1-02608c9eebac}\000A	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\0004	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Properties\{540b947e-8b40-45bc-a8a2-6a0b894cbda2}\0009	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Properties\{78c34fc8-104a-4aca-9ea4-524d52996e57}\005A	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Properties\{78c34fc8-104a-4aca-9ea4-524d52996e57}\005A	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\HardwareID	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0003	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Capabilities	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\HardwareID	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Properties\{540b947e-8b40-45bc-a8a2-6a0b894cbda2}\0009	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Properties\{259abffc-50a7-47ce-af08-68c9a7d73366}\000C	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{b725f130-47ef-101a-a5f1-02608c9eebac}\000A	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Properties\{b725f130-47ef-101a-a5f1-02608c9eebac}\000A	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Properties\{51236583-0c4a-4fe8-b81f-166aec13f510}\007A	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Properties\{cf73bb51-3abf-44a2-85e0-9a3dc7a12132}\0006	C:\Windows\explorer.exe	N/A

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{51236583-0c4a-4fe8-b81f-166aec13f510}\0064	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Capabilities	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{51236583-0c4a-4fe8-b81f-166aec13f510}\007A	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Properties\{259abffc-50a7-47ce-af08-68c9a7d73366}\000C	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Properties\{51236583-0c4a-4fe8-b81f-166aec13f510}\0064	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{259abffc-50a7-47ce-af08-68c9a7d73366}\000C	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\FriendlyName	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Properties\{51236583-0c4a-4fe8-b81f-166aec13f510}\0064	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{540b947e-8b40-45bc-a8a2-6a0b894cbda2}\0009	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Properties\{51236583-0c4a-4fe8-b81f-166aec13f510}\007A	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\ConfigFlags	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\FriendlyName	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Properties\{cf73bb51-3abf-44a2-85e0-9a3dc7a12132}\0006	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\0002	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Properties\{b725f130-47ef-101a-a5f1-02608c9eebac}\000A	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Capabilities	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\0002	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\Capabilities	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001\Properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0002	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000002\Properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0002	C:\Windows\explorer.exe	N/A
Key value queried	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\Disk&Ven_WDC&Prod_WDS100T2B0A\4&215468a5&0&000000\FriendlyName	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_Msft&Prod_Virtual_DVD-ROM\2&1f4adffe&0&000001	C:\Windows\explorer.exe	N/A
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Enum\SCSI\CdRom&Ven_DADY&Prod_HL-DT-ST_DVD+-RW\4&215468a5&0&010000\Properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\0004	C:\Windows\explorer.exe	N/A

Enumerates system info in registry

Description	Indicator	Process	Target
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemManufacturer	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemSKU	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Modifies Internet Explorer settings

adware spyware

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000\Software\Microsoft\Internet Explorer\Toolbar	C:\Windows\explorer.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000\Software\Microsoft\Internet Explorer\Toolbar\Locked = "1"	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000\Software\Microsoft\Internet Explorer\Toolbar\ShellBrowser	C:\Windows\explorer.exe	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000\Software\Microsoft\Internet Explorer\Toolbar\ShellBrowser\ITBar7Layout = 13000000000000000000000020000000100000000000000000010000000107000005e0100	C:\Windows\explorer.exe	N/A

Modifies data under HKEY_USERS

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry\TraceTimeLast = "134170326897063138"	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Modifies registry class

Description	Indicator	Process	Target
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\bing.com\Total = "5173"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify\PastIconsStream = 1400000005000000010001000200000014000000494c200602000400540010001000ffffffff2110ffffffffffffffff424d3600000000000000360000002800000010000000400000000100200000000000000100	C:\Windows\explorer.exe	N/A

Description	Indicator	Process	Target
	00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000005000000420000002a000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000004c000000ae00000042000000000000000000000000 000000000100000075000000c3000000cb000000cb000000cb000000cb000000cb000000cb000000cb0 00000cb000000cb0000006a0000001e000000000000005010101a5232323f28b8b8bf9c9c9c9fee3e3e3 fee3e3e3fee3e3e3fee3e3e3fee0e0e0fea1a1a1fe080808f4131315624f4f5aad060609d90000001800000 07a1f1f1ff5989898f3dbdbdbfce3e3e3fee3e3e3fee3e3e3fee3e3e3fedfdfdffe9c9c9cfe1b1b1bda1c1c1c66 969696a8d6d6d6fa535353f2000000b9000000ec5b5b5bf6999999f7adadadfcb3b3b3edd9d9d9fee3e3e3f ee3e3e3fe9f9f9ffe1d1d1dd8292929749f9f9fb7cdcdcdf9b7b7b7f6848484f6000000f7000000ff7b7b7bfe97 9797fe979797fe979797fa9d9d9df9adadadf09a9a9afb0f0f0feb2121216b989898bab0b0b0ecb1b1b1fcb0 b0b0fd888888fe000000fe000000f86c6c6cfb979797fe979797fe979797fe949494fe6a6a6afe090909eb10 101065858585b0aeaeaef6b0b0b0feafafaffea6a6a6fd3f3f3fee000000bb0000009c2f2f2ff28a8a8afc97979 7fe959595fe696969fe131313d81212126c565656ab898989f5959595f9a1a1a1fe767676f53d3d3df80404 04c6000000250000001a060606be303030f46b6b6bfa656565fe121212da17171774585858ba7e7e7efe7 e7e7efe7e7e7efe797979fe0e0e0ee6000000840000002b0000000000000000000000001e0000009905050 5f4050505f41010106658585 8b77d7d7dfc7e7e7efe7e7e7efe7e7e7efe1f1f1fed000000b90000000c00000 00000000000000000000000003000000490000000cb0000004e191919a15b5b5bfc686868f8686868f85f 5f5ffb222222ee000000ca0000001e0000000000000000000000000000000000000000900000067000000 490000000500000072010101ae0e0e0ecd0e0e0ece020202b6000000830000001e000000000000000000 0000000000000000000000000000000000000009000000030000000000000000400000019000000300000 00310000001f00000006000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000500000004200000002a000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000004c000000ae00000042000000000000000000000000 00000100000075000000c3000000cb000000cb000000cb000000cb000000cb000000cb000000cb00000 0cb000000cb0000006a0000001e000000000000005010101a5232323f28b8b8bf9c9c9c9fee3e3e3fee3 e3e3fee3e3e3fee3e3e3fee0e0e0fea1a1a1fe080808f4131315624f4f5aad060609d90000001800000007a1 f1f1ff5989898f3dbdbdbfce3e3e3fee3e3e3fee3e3e3fee3e3e3fedfdfdffe9c9c9cfe1b1b1bda1c1c1c669696 96a8d6d6d6fa535353f2000000b9000000ec5b5b5bf6999999f7adadadfcb3b3b3edd9d9d9fee3e3e3fee3e 3e3fe9f9f9ffe1d1d1dd8292929749f9f9fb7cdcdcdf9b7b7b7f6848484f6000000f7000000ff7b7b7bfe979797 fe979797fe979797fa9d9d9df9adadadf09a9a9afb0f0f0feb2121216b989898bab0b0b0ecb1b1b1fcb0b0b0f d888888fe000000fe000000f86c6c6cfb979797fe979797fe979797fe949494fe6a6a6afe090909eb1010106 5858585b0aeaeaef6b0b0b0feafafaffea6a6a6fd3f3f3fee000000bb0000009c2f2f2ff28a8a8afc979797fe95 9595fe696969fe131313d81212126c565656ab898989f5959595f9a1a1a1fe767676f53d3d3df8040404c60 00000250000001a060606be303030f46b6b6bfa656565fe121212da17171774585858ba7e7e7efe7e7e7e		

Description	Indicator	Process	Target
	fe7e7e7efe797979fe0e0e0ee6000000840000002b000000000000000000000001e00000099050505f4050505f410101066585858b77d7d7dfc7e7e7efe7e7e7efe7e7e7efe1f1f1fed000000b90000000c00000000000000000000000000000030000004900000cb0000004e191919a15b5b5bfc686868f8686868f85f5f5ffb222222ee000000ca0000001e0000000000000000000000000000000000000000900000067000000490000000500000072010101ae0e0e0ecd0e0e0ece020202b6000000830000001e00000000000000000000000000000000000000000000000000000000900000003000000000000000040000001900000030000000310000001f000000600000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000424d3e000000000000003e00000028000000100000004000000001000100000000000000100000000000000000000000000000000000000000000ffffff00ffff0000fff90000fff10000c0010000800000000000000000000000000000000000000080010000c0030000c0070000c80f0000ffff0000ffff0000ffff0000fff90000fff10000c001000080000000000000000000000000000000000000000000000000080010000c0030000c0070000c80f0000ffff0000ffff00000000000000000000000000000000000000000000000000001000000080000000200000004000000024000000010000000000000000100000000000000		
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\Total\ = "6140"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-1760019844-2681172078-3872633735-798519778-3824819574-1684089895-1452983902\DisplayName = "Chrome Sandbox"	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-1760019844-2681172078-3872633735-798519778-3824819574-1684089895-1452983902\Children	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\cr.sb.odmf5200eafd3ad904629cbb0f87a78a3c7211081fe\Children	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\EdpDomStorage	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Settings\Cache\Content\CachePrefix	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\Sea	N/A

Description	Indicator	Process	Target
		rchHost.exe	
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\EdpDomStorage\www.bing.com	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance\	C:\Windows\explorer.exe	N/A
Key created	\Registry\User\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\NotificationData	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DomStorageState	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\bing.com\Total = "56"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key created	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\Instance\	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\www.bing.com	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU	C:\Windows\explorer.exe	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage	C:\Program Files (x86)\Microsoft\Ed	N/A

Description	Indicator	Process	Target
		ge\Application\msedge.exe	
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings	C:\Windows\explorer.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\www.bing.com\ = "23"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\bing.com\Total = "23"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx = ffffffff	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\PersistedTitleBarData\Microsoft.MicrosoftStickyNotes_8wekyb3d8	C:\Windows\explorer.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\PersistedTitleBarData\Microsoft.MicrosoftStickyNotes_8wekyb3d8 = "1"	C:\Windows\explorer.exe	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.PeopleExperienceHost_cw5n1h2txyewy\ApplicationFrame\Microsoft.Windows.PeopleExperienceHos = 6801000088020000	C:\Windows\explorer.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\Total\ = "990"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\bing.com\Total = "482"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-1760019844-2681172078-3872633735-798519778-3824819574-1684089895-1452983902	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Description	Indicator	Process	Target
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\Total\ = "1023"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify\UserStartTime = "134142267872437866"	C:\Windows\explorer.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\www.bing.com\ = "482"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key created	\REGISTRY\MACHINE\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-2122505878-652277452-2375749442-1000\{698BD76F-81DE-4A81-B4A2-6343F060DDF5}	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\MuiCache	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Settings\Cache\Cookies\CachePrefix = "Cookie:"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\EdpDomStorage\bing.com	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A

Description	Indicator	Process	Target
Set value (data)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx = ffffffff	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance\	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\MACHINE\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-2122505878-652277452-2375749442-1000\{A015C4DA-6C69-40EF-932C-725B940C0AD7}	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\MuiCache	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe	N/A
Key created	\REGISTRY\MACHINE\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-2122505878-652277452-2375749442-1000\{11FF2B17-9102-4406-B9A8-F93683E51097}	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\Total	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\Total\ = "1449"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\Instance\	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings	C:\Windows\explo	N/A

Description	Indicator	Process	Target
		rer.exe	
Set value (str)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Settings\Cache\History\CachePrefix = "Visited:"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\www.bing.com\ = "56"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\www.bing.com\ = "5173"	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\PersistedTitleBarData	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\cr.sb.odmf5200eafd3ad904629cbb0f87a78a3c7211081fe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\EdpDomStorage\Total	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-1760019844-2681172078-3872633735-798519778-3824819574-1684089895-1452983902\Moniker = "cr.sb.odmf5200eafd3ad904629cbb0f87a78a3c7211081fe"	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\TrayNotify\IconStreams = 14000000070000000100010005000000140000005000 3a005c004800660072006500660 05c004e0071007a00760061005c004e006300630051006e0067006e005c005900620070006e0079005c005a007600700065006200660062007300670 05c0042006100720051006500760069007200 5c0042006100720051006500760069007200 2e0072006b0072000000000000000000000000000000000000000000000000000000000000000000000000000000000000000	C:\Windows\explorer.exe	N/A

Description	Indicator	Process	Target
	00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000f50100000000000000000000ea07010 0420061007200510065007600690072000a004100620067002000660076007400610072007100200076 00610000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000100000000000000000000 00000000000000000000000000000000000000000039603be1ae91dc010000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000010000007b005300330038004f00530034003000 34002d003100510034003300 2d0034003200530032002d0039003300300035002d00360037005100520 030004f0032003800530050003200330 07d005c0072006b00630079006200650072006500 2e0072006b 00720000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000002000000ea070100000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000ffffffff75ae2078e323294282c1e41cb67d5b9c00000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000		

Description	Indicator	Process	Target
	00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 30000007b005300330038004f0053003400300034002d0031005100340033002d003400320053003200 2d0039003300300035002d003600370051005200300004f003200380053005000320033007d005c00720 06b006300790062006500720065002e0072006b00720000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000002000000ea070100 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000ffffffff81ae2078e323294282c 1e41cb67d5b9c0000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000020000007b005300330038004f0053003400300034002 d0031005100340033002d0034003200530032002d0039003300300035002d00360037005100520030000 4f0032003800530050003200330007d005c0072006b006300790062006500720065002e0072006b00720 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000002000000ea07010000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000ffffffff82ae2078e323294282c1e41cb67d5b9c0000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000		

Description	Indicator	Process	Target
	00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000010000 007b005300330038004f0053003400300034002d0031005100340033002d0034003200530032002d003 90033003000035002d0036003700510052003000 4f0032003800530050003200330 07d005c0072006b00 6300790062006500720065002e0072006b0072000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000002000000ea07010000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000ffffffff83ae2078e323294282c1e41c b67d5b9c000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000		
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\Instance\	C:\Windows\explorer.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2122505878-652277452-2375749442-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoftwindows.client.cbs_cw5n1h2txyewy\Internet Explorer\DOMStorage\bing.com	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A

Suspicious behavior: AddClipboardFormatListener

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\explorer.exe	N/A

Suspicious behavior: EnumeratesProcesses

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A

Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Suspicious use of AdjustPrivilegeToken

Description	Indicator	Process	Target
Token: SeDebugPrivilege	N/A	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A

Description	Indicator	Process	Target
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Windows\explorer.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Windows\explorer.exe	N/A

Suspicious use of FindShellTrayWindow

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Windows\system32\sihost.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A

Suspicious use of SendNotifyMessage

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A

Suspicious use of SetWindowsHookEx

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A
N/A	N/A	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe	N/A
N/A	N/A	C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe	N/A
N/A	N/A	C:\Windows\explorer.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 3080 wrote to memory of 752	N/A	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4568	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 3136	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2068	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2068	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2068	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4228	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4228	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 244	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 244	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 244	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4900	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4900	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4900	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2728	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Description	Indicator	Process	Target
PID 752 wrote to memory of 4576	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 1568	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 3788	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2728	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2728	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4576	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4576	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 1568	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 1568	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 3788	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 3788	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2680	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2680	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4252	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4252	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 428	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 428	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 428	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4776	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 3372	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4776	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 3372	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2384	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe
PID 752 wrote to memory of 4240	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 4240 wrote to memory of 3964	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\cookie_exporter.exe
PID 752 wrote to memory of 4088	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4088	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 3532	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 3532	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4976	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4972	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4976	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4972	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Description	Indicator	Process	Target
PID 752 wrote to memory of 4508	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4508	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 1540	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4788	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4880	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 5068	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 5068	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2312	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2312	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 2488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4748	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4748	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 4956	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 1964	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 752 wrote to memory of 1964	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Uses Task Scheduler COM API

persistence

Uses Volume Shadow Copy WMI provider

ransomware

Uses Volume Shadow Copy service COM API

ransomware

5. 4. Processes

C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe

```
"C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (6).exe"
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument https://apps.microsoft.com/store/detail/9NKSQGP7F2NH?ocid=&referrer=psi
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=139.0.7258.155 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 --annotation=prod=Edge --annotation=ver=139.0.3405.125 --initial-client-data=0x2e0,0x2e4,0x2e8,0x2dc,0x308,0x7ffa2913c188,0x7ffa2913c194,0x7ffa2913c1a0
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-pre-read-main-dll --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=1836,i,12573967052375700442,471481216202029628 2,524288 --field-trial-handle=2148,i,790476596251690310 0,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=2172 /prefetch:11
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-pre-read-main-dll --force-high-res-
timeticks=disabled --gpu-
preferences=SAAAAAAAAADgAAAIAAAAAAAAAAAAAGAAAQAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --
always-read-main-dll --metrics-shmem-handle=1536,i,5244017260197807560,7717615650134679340,262144 --field-trial-
handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=2144 /prefetch:2
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US
--service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=2480,i,14047423372957724612,5575127233576330789,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 -
-variations-seed-version --mojo-platform-channel-handle=2616 /prefetch:13
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\elevation_service.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\elevation_service.exe"
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --
video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=4 --enable-main-
frame-before-activation --renderer-client-id=6 --always-read-main-dll --metrics-shmem-
handle=3500,i,17529577636760993815,4609878101320864938,2097152 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144
--variations-seed-version --mojo-platform-channel-handle=3572 /prefetch:1
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --
video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=4 --enable-main-
frame-before-activation --renderer-client-id=5 --always-read-main-dll --metrics-shmem-
handle=3504,i,9967861958152927349,5651998649515985980,2097152 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 -
-variations-seed-version --mojo-platform-channel-handle=3580 /prefetch:1
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --
video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=4 --enable-main-
frame-before-activation --renderer-client-id=7 --always-read-main-dll --metrics-shmem-
handle=4140,i,14554233213303693690,12465207651948607446,2097152 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144
--variations-seed-version --mojo-platform-channel-handle=4156 /prefetch:1
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --extension-process --renderer-sub-type=extension --pdf-
upsell-enabled --force-high-res-timeticks=disabled --video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --
device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=8 --always-read-main-dll --metrics-
shmem-handle=4124,i,15722381340749080516,16332278697192484837,2097152 --field-trial-
handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4204 /prefetch:9
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --extension-process --renderer-sub-type=extension --pdf-
upsell-enabled --force-high-res-timeticks=disabled --video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --
device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=10 --always-read-main-dll --
metrics-shmem-handle=4192,i,220588454743764970 2,5618225755785116146,2097152 --field-trial-
handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4224 /prefetch:9
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --
video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=4 --enable-main-
frame-before-activation --renderer-client-id=9 --always-read-main-dll --metrics-shmem-
handle=4160,i,16200841809992124405,6717661925089393684,2097152 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144
--variations-seed-version --mojo-platform-channel-handle=4132 /prefetch:1
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=PooledProcess2 --lang=en-US --service-
sandbox-type=utility --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=4540,i,74967512567150007 58,17178038229154291714,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 -
-variations-seed-version --mojo-platform-channel-handle=4492 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=PooledProcess2 --lang=en-US --service-
sandbox-type=utility --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=3616,i,15970994273501691 05,296469557319807572,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --
variations-seed-version --mojo-platform-channel-handle=5428 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=15 --always-read-main-dll --metrics-shmem-handle=5536,i,7447862188891505679,14780221396520158775,2097152 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5556 /prefetch:1
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.mojom.AssetStoreService --lang=en-US --service-sandbox-type=asset_store_service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5692,i,254131882937008768,15217204857717274636,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5768 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity_extraction_service.mojom.Extractor --lang=en-US --service-sandbox-type=entity_extraction --onnx-enabled-for-ee --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5696,i,12110304684372738244,11825696478884792562,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5788 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6520,i,10357666702562224623,5278543944714543303,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=3820 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6520,i,10357666702562224623,5278543944714543303,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=3820 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.ProfileImport --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=3864,i,15979672797402796706,3475165007963864902,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4272 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\cookie_exporter.exe

```
cookie_exporter.exe --cookie-json=1136
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5124,i,2856052111916626370,5425987247789258996,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5044 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5056,i,4526393783540615998,10905350975836104729,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5124 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5104,i,2322237325972651275,160979507302579763,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=3872 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6556,i,3131587077165658515,10610936769953809699,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4272 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=PooledProcess2 --lang=en-US --service-sandbox-type=utility --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6804,i,4124817489847135089,10019866661389730213,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5068 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --message-loop-type-ui --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=3844,i,4920165839654374074,5908357317888284636,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4332 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --message-loop-type-ui --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=3836,i,10293534164122278625,9570683311893990463,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4084 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --message-loop-type-ui --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=3832,i,17203509090241141270,5071782973275300051,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4496 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_search_indexer.mojom.SearchIndexerInterfaceBroker --lang=en-US --service-sandbox-type=search_indexer --message-loop-type-ui --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5840,i,8054002799403472891,15541357790458089631,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5916 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5412,i,8941838033006634203,9251501865187550028,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5468 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=1908,i,3228098085744026991,948018832581304285,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4208 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=836,i,8852072178002096820,15481081157907559080,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5700 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --disable-gpu-sandbox --use-gl=disabled --gpu-vendor-id=5140 --gpu-device-id=140 --gpu-sub-system-id=0 --gpu-revision=0 --gpu-driver-version=10.0.22000.1 --force-high-res-timeticks=disabled --gpu-preferences=SAAAAAAAAADoAAAIAAAAAAAAAAAAAGAAAQAAAAAAAACEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAIAAAAAAAAAA== --always-read-main-dll --metrics-shmem-handle=4576,i,17023052798754554327,4596620425639590696,262144 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=836 /prefetch:10
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6204,i,2064640120541923667,4824768315878007596,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4492 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6588,i,735064803440493343,15831539379887494338,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=6048 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=on_device_model.mojom.OnDeviceModelService --lang=en-US --service-sandbox-type=on_device_model_execution --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4060,i,3078174015715571275,12568185244815222504,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5276 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.mojom.AssetStoreService --lang=en-US --service-sandbox-type=asset_store_service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6568,i,2606407061745557799,2967838625652968991,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=5084 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=on_device_model.mojom.OnDeviceModelService
--lang=en-US --service-sandbox-type=on_device_model_execution --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=3440,i,4956795967843743928,5853972878986737061,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --
variations-seed-version --mojo-platform-channel-handle=4604 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --
service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=6976,i,5798540459438444056,12117359867124995675,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 -
-variations-seed-version --mojo-platform-channel-handle=5444 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --
service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=6204,i,16053736510308974163,12173698689174669708,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144
--variations-seed-version --mojo-platform-channel-handle=6796 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --
service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=3216,i,3033507544603849225,11691941013528722755,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 -
-variations-seed-version --mojo-platform-channel-handle=5812 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.mojom.AssetStoreService --
lang=en-US --service-sandbox-type=asset_store_service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=7052,i,15634875338573715020,1931351723996994376,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 -
-variations-seed-version --mojo-platform-channel-handle=4592 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-
type=edge_xpay_wallet.mojom.EdgeXPayWalletService --lang=en-US --service-sandbox-type=utility --force-high-res-timeticks=disabled --always-
read-main-dll --metrics-shmem-handle=3516,i,7675147976178060256,8958987946081364270,524288 --field-trial-
handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=7092 /prefetch:14
```

C:\Windows\system32\sihost.exe

```
sihost.exe
```

C:\Windows\explorer.exe

```
explorer.exe
```

C:\Windows\explorer.exe

```
explorer.exe /LOADSAVEDWINDOWS
```

C:\Windows\explorer.exe

```
explorer.exe
```

C:\Windows\System32\rundll32.exe

```
C:\Windows\System32\rundll32.exe shell32.dll,SHCreateLocalServerRunDll {9BA05972-F6A8-11CF-A442-00A0C90A8F39} -Embedding
```

C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe

```
"C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe" -
ServerName:CortanaUI.AppXstmwaab17q5s3y22tp6apqz7a45vwv65.mca
```

C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe

```
"C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -
ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --
service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=3436,i,702359790733077199,14952744703485303721,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --
variations-seed-version --mojo-platform-channel-handle=5752 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --
service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=2588,i,702739783572700850,11292028287445750006,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --
variations-seed-version --mojo-platform-channel-handle=5332 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4968,i,4637591659113545786,3543568532613773552,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=6696 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6156,i,16106134954496562852,3463763453120293229,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=7040 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5428,i,10637925836797684001,11457393483420800452,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=4564 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.mojom.AssetStoreService --lang=en-US --service-sandbox-type=asset_store_service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4688,i,5231228843155741863,12767675072600876845,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=7064 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4484,i,11775023361714397105,11197665590019310493,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=7068 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4528,i,11158910319574123318,4871030923434045182,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=7044 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4528,i,4866932430476708822,16182030965428343410,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=6848 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4656,i,4507375112275364585,10302890424506153665,524288 --field-trial-handle=2148,i,7904765962516903100,15868068998233072447,262144 --variations-seed-version --mojo-platform-channel-handle=7044 /prefetch:14
```

5. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	storeedge.microsoft.com	udp
GB	104.83.3.113:443	storeedge.microsoft.com	tcp
GB	2.19.14.44:443	store-images.microsoft.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	apps.microsoft.com	udp
US	8.8.8.8:53	apps.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	clients2.google.com	udp
US	8.8.8.8:53	clients2.google.com	udp
GB	142.250.129.113:443	clients2.google.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	150.171.109.209:443	apps.microsoft.com	tcp
US	150.171.28.11:80	edge.microsoft.com	tcp
US	8.8.8.8:53	copilot.microsoft.com	udp
US	8.8.8.8:53	copilot.microsoft.com	udp
US	150.171.109.209:443	apps.microsoft.com	tcp
GB	142.250.129.113:443	clients2.google.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp

US	104.18.22.222:443	copilot.microsoft.com	udp
US	104.18.22.222:443	copilot.microsoft.com	tcp
US	150.171.109.209:443	apps.microsoft.com	tcp
US	8.8.8.8:53	clients2.googleusercontent.com	udp
US	8.8.8.8:53	clients2.googleusercontent.com	udp
GB	142.250.117.132:443	clients2.googleusercontent.com	tcp
US	8.8.8.8:53	msedgeextensions.sf.tlu.dl.delivery.mp.microsoft.com	udp
US	8.8.8.8:53	msedgeextensions.sf.tlu.dl.delivery.mp.microsoft.com	udp
GB	2.20.12.82:443	msedgeextensions.sf.tlu.dl.delivery.mp.microsoft.com	tcp
US	8.8.8.8:53	images-eds-ssl.xboxlive.com	udp
US	8.8.8.8:53	images-eds-ssl.xboxlive.com	udp
US	8.8.8.8:53	sparkcdneus2.azureedge.net	udp
US	8.8.8.8:53	sparkcdneus2.azureedge.net	udp
US	8.8.8.8:53	musicart.xboxlive.com	udp
US	8.8.8.8:53	musicart.xboxlive.com	udp
US	8.8.8.8:53	wcpstatic.microsoft.com	udp
US	8.8.8.8:53	wcpstatic.microsoft.com	udp
GB	2.19.12.9:443	musicart.xboxlive.com	tcp
US	8.8.8.8:53	store-images.microsoft.com	udp
US	8.8.8.8:53	store-images.microsoft.com	udp
GB	2.19.12.9:443	musicart.xboxlive.com	tcp
US	150.171.109.210:443	wcpstatic.microsoft.com	tcp
GB	2.19.14.44:443	store-images.microsoft.com	tcp
US	8.8.8.8:53	www.clarity.ms	udp
US	8.8.8.8:53	www.clarity.ms	udp
US	8.8.8.8:53	js.monitor.azure.com	udp
US	8.8.8.8:53	js.monitor.azure.com	udp
CH	20.250.198.32:443	www.clarity.ms	tcp
US	150.171.109.213:443	js.monitor.azure.com	tcp
US	150.171.109.213:443	js.monitor.azure.com	tcp
US	150.171.109.213:443	js.monitor.azure.com	tcp
US	150.171.109.213:443	js.monitor.azure.com	tcp
CH	20.250.198.32:443	www.clarity.ms	tcp
US	150.171.109.209:443	apps.microsoft.com	tcp
US	8.8.8.8:53	login.microsoftonline.com	udp
US	8.8.8.8:53	login.microsoftonline.com	udp
NL	20.190.160.22:443	login.microsoftonline.com	tcp
US	8.8.8.8:53	login.microsoftonline.com	udp
US	8.8.8.8:53	login.microsoftonline.com	udp
NL	40.126.32.138:443	login.microsoftonline.com	tcp
GB	92.123.128.144:443	www.bing.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	scripts.clarity.ms	udp
US	8.8.8.8:53	scripts.clarity.ms	udp
US	150.171.109.209:443	apps.microsoft.com	tcp
US	150.171.109.214:443	scripts.clarity.ms	tcp
US	8.8.8.8:53	browser.events.data.microsoft.com	udp
US	8.8.8.8:53	browser.events.data.microsoft.com	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	52.168.112.67:443	browser.events.data.microsoft.com	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	150.171.109.209:443	apps.microsoft.com	tcp
GB	92.123.128.144:443	www.bing.com	udp
US	52.168.112.67:443	browser.events.data.microsoft.com	tcp
US	8.8.8.8:53	northcentralus-0.in.applicationinsights.azure.com	udp
US	8.8.8.8:53	northcentralus-0.in.applicationinsights.azure.com	udp
US	52.240.245.67:443	northcentralus-0.in.applicationinsights.azure.com	tcp
US	8.8.8.8:53	edgeassetservice.azureedge.net	udp
US	8.8.8.8:53	edgeassetservice.azureedge.net	udp
US	150.171.109.215:443	edgeassetservice.azureedge.net	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.28.11:443	edge.microsoft.com	tcp
N/A	224.0.0.251:5353		udp
US	150.171.28.11:443	edge.microsoft.com	tcp

US	8.8.8.8:53	edge-consumer-static.azureedge.net	udp
US	8.8.8.8:53	edge-consumer-static.azureedge.net	udp
US	150.171.109.216:443	edge-consumer-static.azureedge.net	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	199.232.210.172:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
GB	142.251.30.94:80	c.pki.goog	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	8.8.8.8:53	static.edge.microsoftapp.net	udp
US	8.8.8.8:53	static.edge.microsoftapp.net	udp
US	150.171.109.211:443	static.edge.microsoftapp.net	tcp
US	8.8.8.8:53	edge-mobile-static.azureedge.net	udp
US	8.8.8.8:53	edge-mobile-static.azureedge.net	udp
US	8.8.8.8:53	edge-cloud-resource-static.azureedge.net	udp
US	8.8.8.8:53	edge-cloud-resource-static.azureedge.net	udp
US	150.171.109.215:443	edge-cloud-resource-static.azureedge.net	tcp
US	150.171.109.210:443	edge-mobile-static.azureedge.net	tcp
GB	90.244.159.107:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
GB	92.123.128.182:443	www.bing.com	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	172.171.87.38:443	y.clarity.ms	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	edgeassetservice.azureedge.net	udp
US	8.8.8.8:53	edgeassetservice.azureedge.net	udp
US	150.171.109.216:443	edgeassetservice.azureedge.net	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
GB	90.244.159.107:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	172.171.87.38:443	y.clarity.ms	tcp
GB	92.123.128.148:443	www.bing.com	udp
GB	92.123.128.148:443	www.bing.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	172.171.87.38:443	y.clarity.ms	tcp
US	8.8.8.8:53	xpaywalletcdn-prod.azureedge.net	udp
US	8.8.8.8:53	xpaywalletcdn-prod.azureedge.net	udp
US	150.171.109.212:443	xpaywalletcdn-prod.azureedge.net	tcp
GB	92.123.128.172:443	www.bing.com	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
US	8.8.8.8:53	edge.microsoft.com	udp

US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	y.clarity.ms	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	172.171.87.38:443	y.clarity.ms	tcp
US	8.8.8.8:53	y.clarity.ms	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	172.171.87.38:443	y.clarity.ms	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	172.171.87.38:443	y.clarity.ms	tcp
GB	90.244.159.107:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	8.8.8.8:53	y.clarity.ms	udp
US	172.171.87.38:443	y.clarity.ms	tcp
US	172.171.87.38:443	y.clarity.ms	tcp
GB	90.244.159.107:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	edgeassetservice.azureedge.net	udp
US	8.8.8.8:53	edgeassetservice.azureedge.net	udp
US	150.171.109.216:443	edgeassetservice.azureedge.net	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
GB	90.244.159.107:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
GB	2.20.12.101:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
GB	2.20.12.101:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.28.11:443	edge.microsoft.com	tcp

5. 6. Files

memory/3080-0-0x000001E527B90000-0x000001E527CA2000-memory.dmp

memory/3080-1-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-2-0x000001E529AD0000-0x000001E529ADA000-memory.dmp

memory/3080-3-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-4-0x000001E542C80000-0x000001E542D3A000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\Tmp291E.tmp

MD5	a10f31fa140f2608ff150125f3687920
SHA1	ec411cc7005aaa8e3775cf105fcd4e1239f8ed4b
SHA256	28c871238311d40287c51dc09aee6510cac53063299817770716 00b1112286c6
SHA512	cf915fb34cd5ecfbd6b25171d6e0d3d09af2597edf29f9f24fa474685d4c5ec9bc742ade9f29abac457dd645ee955b1914a635c90af77c519d2ada895e7ecf12

memory/3080-15-0x000001E542BE0000-0x000001E542BF2000-memory.dmp

memory/3080-16-0x000001E542C40000-0x000001E542C7C000-memory.dmp

memory/3080-17-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-18-0x000001E542D40000-0x000001E542D66000-memory.dmp

memory/3080-19-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-21-0x000001E5430A0000-0x000001E5430AE000-memory.dmp

memory/3080-20-0x000001E545440000-0x000001E545478000-memory.dmp

memory/3080-22-0x000001E543280000-0x000001E543288000-memory.dmp

memory/3080-23-0x000001E545D20000-0x000001E545EA8000-memory.dmp

memory/3080-29-0x000001E545BA0000-0x000001E545BA8000-memory.dmp

memory/3080-30-0x000001E542450000-0x000001E542460000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\Microsoft.Services.Store.winmd

MD5	4aae69886cd900c373d69194dc4241a0
SHA1	50cc74acbfedea48f1225181682253002bced6da
SHA256	44f3a05334de6ca0b43ebd17f6c7f1935630e026f049f28828566e364b7f41aa
SHA512	02289cb11b4090028c5a2fecc69be1ddb8ed0b57125c3c7d898b9937b46da53dcfd3cd7c601c8f7e124f5587ff0a3f4450fa7da0add5abab4ff3903ab23f82c8

memory/3080-35-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-36-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-37-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-38-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-39-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-41-0x000001E5280D0000-0x000001E5280DC000-memory.dmp

memory/3080-40-0x000001E5280C0000-0x000001E5280C8000-memory.dmp

memory/3080-42-0x000001E529B10000-0x000001E529B22000-memory.dmp

memory/3080-43-0x000001E542450000-0x000001E542460000-memory.dmp

memory/3080-48-0x000001E5280D0000-0x000001E5280DC000-memory.dmp

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\settings.dat

MD5	9093390d9e798f9a4ccc25251c10fea5
SHA1	96837bd82509feb4ca69a53466162950148f0394
SHA256	7173f2853e3b591f142ed047bb6a2ea62d5d817f9016fdd31efbebd88f820e91
SHA512	4db01b0d83eba59662ef7f147a96bb0034c92f2c5d5ac83ceeae12ddc800fe8dbce64d41320c2a3031796e981edc605460e3a1da207a6a9d39812740085a86ef

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Local State

MD5	b092b7a9152517edb283ca081d81023d
SHA1	68963cfa68e2c6433f3027450752fee013bd2a9e
SHA256	6a506d9bdc741d6d97f07d4f62d36d4dc494b721ed22eeadbb39e7a08ac0dfdc
SHA512	f4a9f6177d1f98b88823b54dc72dfcb7103523bf7d8a41ed69937b84b7924954c58cd087169789c10bb59143d4af5cc6dd05172f2964b4f0432d98b523b1ef2b

\??\pipe\crashpad_752_JEFDMVEQNTTTKIBR

MD5	d41d8cd98f00b204e9800998ecf8427e
SHA1	da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA512	cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\settings.dat

MD5	35b0754e7f5b0bef0f59e6474c3c9e30
SHA1	a5dbcd61883043544b184e46e47beb3bf5d259a8
SHA256	eacd218daf22fcefbc23ae70ce919d8ac95b89c3f7d038f647296c47a218fc46
SHA512	0a14f00d3bf385bd104004e3adb021fc5b135483b30669a0f446d235f67bf00d734e76a56ac18adc3d6765163a992c78b2c6833f0e764506a9c06ff2ad8fc90e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Local State

MD5	74521e64e1a9f06f574ed19046d9186c
SHA1	784157a02cccddbf69d4a9494ad97b45a601aac3
SHA256	bee314ab3c2bab1f5b3c6429c9cfd20e04238bbe1e04f769b0c2b710bdba22a8
SHA512	a320d33bd6072887b0d96b57eb7bc63935da093930add59a39ed986aef1ef47e977b0cd75d856632eac89290a4e8bad024a0355b929f72b04662856489 64f0ed

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Edge Profile.ico

MD5	efe54a870e0f5ff28d7e00036b861065
SHA1	10663a71c9815382ca5a1689dfcebe737c557b1d
SHA256	31a226211c491e1b0832d4cd3cf34d97165e24a7ce4ec655259cd188f3a2bd88
SHA512	4d7ed9d3e22a58f0e169c9200e351d3a938c82ab7920567f67bf29d33b28192329ea05657d1077aebaf2c2b5151eb50c84e5ab590733ff824389566d93381c01

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports

MD5	d751713988987e9331980363e24189ce
SHA1	97d170e1550eee4afc0af065b78cda302a97674c
SHA256	4f53cda18c2baa0c0354bb5f9a3ecbe5ed12ab4d8e11ba873c2f11161202b945
SHA512	b25b294cb4deb69ea00a4c3cf3113904801b6015e5956bd019a8570b1fe1d6040e944ef3cdee16d0a46503ca6e659a25f21cf9ceddc13f352a3c98138c15d6af

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\index.txt

MD5	8536423d057127ef2f686f911a62e4ba
SHA1	8e2da87d7236a60a0abc64f1db0797bbf9a61622
SHA256	cbe665f85f98ee38ff2dbb7de5bcaae64164f57df8ff64892eb637edb98ce39d
SHA512	b6c81dd72d69517c07273d180d70bb1d2ba78463f835fb6eea3e36712f99049ba5dd631d0d9ba19e57b41e4687d0a17c01a7a3e72dc111e74668f6f526b71777

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\index.txt~RFe586c61.TMP

MD5	7bab79ae4ea2bb407c658cb23ac6a1e7
SHA1	480a4afd2c0a303fb492b325a6e40df8dd4d91f3
SHA256	5febc6ba6226dcc5d9a42dc8adcf0cb13c09544370025e950939e21a722b82a5
SHA512	fc148b7b9526ccde7698a52a5ab038ecdd73df791c69c5140db701ab2b46c6e23fc7d4b99f326872877519fe9fb78db33a1b5eb568197b2721e32cda10478a81

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps

MD5	25dca813dd764f2197142ef84bc5ce66
SHA1	8d6aefb01ee9f6d1fb0cfd89326cfe35af53a53d
SHA256	eb2fd7422436fff93f6be09df3294b26cdb7afd18e6aa94dcdc0f208db78b2ed
SHA512	a9c8cd547c874b7b69cbb3a0c8214f43837911e522db768dcd075d23d05acfd7122cf2bcad281ea745025e4fb67cc9061b79f9dc1288ac1a113bd0d961841d43

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\dcaajljecejllikfgbhjdgeognacjkkp\MANIFEST-000001

MD5	5af87dfd673ba2115e2fcf5cfdb727ab
SHA1	d5b5bbf396dc291274584ef71f444f420b6056f1
SHA256	f9d31b278e215eb0d0e9cd709edfa037e828f36214ab7906f612160fead4b2b4
SHA512	de34583a7dbafe4dd0dc0601e8f6906b9bc6a00c56c9323561204f77abbc0dc9007c480ffe4092ff2f194d54616caf50aecbd4a1e9583cae0c76ad6dd7c2375b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\dcaajljecejllikfgbhjdgeognacjkkp\CURRENT

MD5	46295cac801e5d4857d09837238a6394
SHA1	44e0fa1b517dbf802b18faf0785eeea6ac51594b
SHA256	0f1bad70c7bd1e0a69562853ec529355462fcd0423263a3d39d6d0d70b780443
SHA512	8969402593f927350e2ceb4b5bc2a277f3754697c1961e3d6237da322257fbab42909e1a742e22223447f3a4805f8d8ef525432a7c3515a549e984d3eff72b23

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\Logs\sync_diagnostic.log

MD5	0eb41b8e6e5c83bf153ff6568208640f
SHA1	904baf9409a13ac15501d0286cdbf091f7edab3f
SHA256	011c5217d4e3922895665b0d7fc1362134bc4983e7d27e65475a6a6bb5c53f18
SHA512	5201812979630d1bc8278e8c6071deb565d1443003808297048322c9bb13d7f5918579aacf0aea54d7dda510e27106078b3a7e01c48c3c08df7ae6791a9d7fbd

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\DualEngine\SiteList-Enterprise.json

MD5	99914b932bd37a50b983c5e7c90ae93b
SHA1	bf21a9e8fbc5a3846fb05b4fa0859e0917b2202f
SHA256	44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
SHA512	27c74670adb75075fad058d5ceaf7b20c4e7786c83bae8a32f626f9782af34c9a33c2046ef60fd2a7878d378e29fec851806bbd9a67878f3a9f1cda4830763fd

C:\Users\Admin\AppData\Local\Temp\scoped_dir752_746393983\c496939a-e710-41a4-9b44-d8d598ce6281.tmp

MD5	98144a4b67ce21832c45a0d20d3163fc
SHA1	d5d7d718eb78e4332899326f111796da8604a2d3
SHA256	31e3cb755cf2d66510c7f94c42df615dc13575ad2e8fd5a63887ca145424d34e
SHA512	3e25330d1ce5810426da57aff275d2ecdd09b6c0cbe4f7534cf8bf17c39f595dcca147b204b6f74396b23160757cc030753c4c227b0dbea54f489b9016459ae8

C:\Users\Admin\AppData\Local\Temp\61c5fce2-1223-4dfe-b4c0-8044bc98850a.tmp

MD5	5058f1af8388633f609cadb75a75dc9d
SHA1	3a52ce780950d4d969792a2559cd519d7ee8c727
SHA256	cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8
SHA512	0b61241d7c17bcbb1baee7094d14b7c451efecc7ffcbd92598a0f13d313cc9ebc2a07e61f007baf58fbf94ff9a8695bdd5cae7ce03bbf1e94e93613a00f25f21

C:\Users\Admin\AppData\Local\Temp\88fb35cb-56d2-49dd-812a-996eed616a3a.tmp

MD5	78e47dda17341bed7be45dccfd89ac87
SHA1	1afde30e46997452d11e4a2adbbf35cce7a1404f
SHA256	67d161098be68cd24febc0c7b48f515f199dda72f20ae3bbb97fcf2542bb0550
SHA512	9574a66d3756540479dc955c4057144283e09cae11ce11ebce801053bb48e536e67dc823b91895a9e3ee8d3cb27c065d5e9030c39a26cbf3f201348385b418a5

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\BookmarkMergedSurfaceOrdering

MD5	377d072e137022223a370760763420bb
SHA1	534e5f914ae99bf0a342a2f7a7e0724bd0d11ef7
SHA256	4489f9e3e454748b3521eb214e0a5694d562cff3d9ff511cb456953c8f534c00
SHA512	d1e37e45e8d603c46c9254d7295744104222b09340246c5e5f50d661d4688ccc2068adf1e0cd78599bcdcf475f8a0a6255dcd3e429812aa14cc2e2022309955c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\settings.dat

MD5	9441eb918c6d8a3adf2fcea5c9885831
SHA1	1a6a33c8c02fa0dd43450117551d460848b4290b
SHA256	386b98dfeed9fd04554c22875f1a73fe0e1481d3005a1c5a9f3a10f991af62b8
SHA512	3f74edbe5eca2dd845d131b097f1d6c804b6051c1f4881ed1cfbc3b1f69830b00d8466f65b39e5cded6f6fb5aa63e10f61c3fabb0fb4a8a7730769ee8c0e560c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Ad Blocking\blocklist

MD5	433cd7e7c552800420dbba04318f3078
SHA1	07950a895d62a0a61a71b4042d3d366a9c832a7f
SHA256	5b0a1dcb499af22b48e1eaab3a5103eaa6f5ac93f980c39104034a374163190f
SHA512	640f89c3bd91d0fbd71d7054d728094ab51c72b1dfdc93c8adcb110a2541a8da3f1c7811cc9d78aa4cfe010d1de2002af132860ea0cf3d77a2a6fbbc1af561b9

C:\Users\Admin\AppData\Local\Temp\scoped_dir752_512392696\CRX_INSTALL\content_new.js

MD5	3de1e7d989c232fc1b58f4e32de15d64
SHA1	42b152ea7e7f31a964914f344543b8bf14b5f558
SHA256	d4aa4602a1590a4b8a1bce8b8d670264c9fb532adc97a72bc10c43343650385a
SHA512	177e5bdf3a1149b0229b6297baf7b122602f7bd753f96aa41ccf2d15b2bcf6af368a39bb20336ccce121645ec097f6bedb94666c74acb6174eb728fbfc43bc2a

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Secure Preferences

MD5	611f29071130cd6613468b2fd0ce9541
SHA1	54cd372e4f5f08fcc5d1494bd977681a9df22182
SHA256	e1ae75affc467e67b26566d640c363f3e4ac267e91a95c90de26aee07c2fd547
SHA512	93ef28fe250c007a4425168f6a14ffa84c957791119d4b5d608b08c6e6488191b7d4dcc3e4008624395806f406c1fbe75ef334640aad99eb930386068fb14d3f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences

MD5	d7d9b381dde68a8565ea39d2fe9bd924
SHA1	8e28e01e299e4b844e9295a5afac563d017330d7
SHA256	e57ce622134e7d098b570f7b1d150b7be9aecf1223706697da3f096072c5d452
SHA512	92c54f26487c02395a64394373b89ea24646601e9b7ca512564b9c905b9cddae679803f94a038aeff22788b2e3f99cf85ec1736c294d249a4808b7d428cab741

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Local State

MD5	a43d88425201e6dfb70e96d89ab080c5
SHA1	a29a2822e34050a0048ec2c4831577f9cc580d71
SHA256	c3afbd745d46ba1a121501b84ed6043bf85ff1f13ef32d9ad9cc74dad97f6c47
SHA512	4ebc2bab393a302a63994efa6afd03f4d26088a8e15a3fc9eb8a020d971a0aa54b0c4ff2f7810b7da5464da4153598f90582343aeb203f0371c045c8efc69ec7

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\extensions_crx_cache\0b5bee83-e55f-4b61-aac4-187a26a3ab79.tmp

MD5	2aa9e263ee3796d9ce358460a2451b4c
SHA1	7a55d937c0cd1f7543a12be730e4a78d0a14a545
SHA256	2771d13c637c267132afff9db67537bef95708534b79ae8d954254c4e64e4e0f
SHA512	4909e73ffd1a777a9f102a8831f6ae5a9091084a2755707363251f39164bb65e22c318972ea59e7155976c6a626691dfa94539ee752f58e31aa16f4de5cdbccf

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State

MD5	285252a2f6327d41eab203dc2f402c67
SHA1	acedb7ba5fbc3ce914a8bf386a6f72ca7baa33c6
SHA256	5dfc321417fc31359f23320ea68014ebfd793c5bbed55f77dab4180bbd4a2026
SHA512	11ce7cb484fee66894e63c31db0d6b7ef66ad0327d4e7e2eb85f3bcc2e836a3a522c68d681e84542e471e54f765e091efe1ee4065641b0299b15613eb32dcc0d

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index

MD5	b52a590bfbcf747cba58fa2c0fa6f1a1
SHA1	0d51a1e77d215a3a558b1bdb1a8599197172888f
SHA256	bc5b686e46000ad993f93e8c335a889b434a24e18144e16d360b40343ff42503
SHA512	c87b5ffcdda283e0b26c47e03c9f5663b387d56a7e0e0229d255ff311807fed135c6d49404548daf0cb63778ea5ed1314e5db04067fc2a61c3829ab6dae3dab3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index~RFe58ba52.TMP

MD5	8e21fbb5744444c71acd696a62374ddd
SHA1	5f01d2002fd7e09f3bb239a2e5875f4ee1eb6cfb
SHA256	e1899b8f98215ecf3d1f8f74e90ccc0bf408ddd704ef38c739959127eeffb021
SHA512	7f93e52242ae1cecb9a71360080623cb351104fada32cef4e1e5975a752eac89be9dd8ceefa266c2671e17455bf2c5e44c3f2f4625a43dc8dbcb1bc78edffb7f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\741256d1-86e0-4e8d-ba43-049b801e663c\index-dir\the-real-index

MD5	c55edac28cd1f45b4acf566665e169b1
SHA1	0a4fa6845d603cfbf99cb88c0bee432cbab7c580
SHA256	18e5f858e838615c35c708fb6c50186f5a5e7218b7fa8e7a1a3d5770bf9ab734
SHA512	a9df87f0ad84fa98c59d9c76e44d1b269aabf3a81a863b6852ccb9b1a5e8336d3c46ecfcd4462ae7f2b2e7cc375a89ece544d9a45866ff8dd3483c223e370a3a

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\741256d1-86e0-4e8d-ba43-049b801e663c\index-dir\the-real-index~RFe58bacf.TMP

MD5	fb4a8a7b38cf663f7432670d1711b0ed
SHA1	5ec37fd8e20b054c16007305aa2b73bf0035d273
SHA256	42b706c6fc914771ddd6463d1b1e0cd1524e4ed1442418fbc9afcf4722131eb7
SHA512	22cdd028596ee0b3360b629ae45b413362e12465ea31ccc564a143f2dd0f4bc4e7f783969c546715e0c2782094110008e5e1542fca87ad32757494a7d2cae90f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index

MD5	b34ca78a63423e0bd7fe1185139824a6
SHA1	b7a2f4830ca6f42446c25484986918ea54e9ca0e
SHA256	10479cefc0483f102a19e2f58146046295da383efacd2b9ee3d2ea7cf5648f69
SHA512	656ac7b2e18ad1fb6605a9fd5fa259ee7ab26c2bdb004b97fb27975e9b649262b1c0d383eabfa93faa977bfc173ddda6a2d9ab22ff6c1943e31da879cd36b3a3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index~RFe58ce09.TMP

MD5	6d515231236612189082868 4af27a1c6
SHA1	0f5028a7facba38384c0c522335e00aea4a27437
SHA256	a8356ddbdbd89ac69a2208c70d2c23390aba92b3f3fd8bfe22ce6122b81a5882
SHA512	bddea60fed3d4d18db7ba3fb01b4a401be84c15fb6ff7794770f1b945c720bc863e200026da214d9cc56b352f59daa9dca4cd0a781d28497b0e8f84182c218fd

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\455d441d-2e76-4e03-a05f-fa225666d693\index-dir\the-real-index~RFe58d0c8.TMP

MD5	9c42ea82a990419fb8865520549c2910
SHA1	16fc483ea9833df42e6c808456c147f22c8bba96
SHA256	294821b39ef395d6d366a40d1e08e7db18d8446509b2c3cdb08ecd6e7474191a
SHA512	2751c1d0973ce2b1081ad9e30695351088ba28ad293e06cce8c925309c2b5d79e485421c8f65d9060b9b4228fdbc7273e1635572d0570844d227bfb2375c39ae

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\455d441d-2e76-4e03-a05f-fa225666d693\index-dir\the-real-index

MD5	0fa41942a4fa50eafafd7f8740aa8009
SHA1	49e1f65614faa602da047ea72ebf6c9873184510
SHA256	5143376c5f06b7c1f6e30e02ed4aeb486488cc9b8dcb467c848ddcb829e68d73
SHA512	08c35e8e7d5534b6ef678cfca8c5b33ddaf030d346a64795e05be52fef3776d3a2cee13622a6e0b42f91d0a3787ae2af9effd3b003b3c1767a64cb0714c2d732

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\index.txt

MD5	850f43585b46facc6536f5ccbb67d31a
SHA1	b98e7bccb2cf266b1da10ba19b8e907a499f8613
SHA256	b423f0b04156e00fcfaeff90e2b516bed9aa88453211518d55359833dad47f19
SHA512	56c8666bcdb54a276a923312461bcda184157f78b245b272db27f6956650109a3ab92e03b7b011f0a6be70932098f359c7e93f3b9f26d04348a4b4de6460ced6

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Local State

MD5	34e51b449e5b5c9ea5e87e7d3ca79e37
SHA1	cf6628f3e3553b8d15a12c3c9b5f07f4e85926c3
SHA256	5fb36c91b41ed044fb4b8ee39154b28721112906c13eceafd26a09fcddc8e74e
SHA512	5ad9f327da6d251034cfef31183204fa2deb2a35accecfe470a6875da58539887d9bf28b2d9617b4bf9afb223c167332a321843eaa078abe2df1758de8a5b235

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Edge Cloud Config\OperationConfig

MD5	f768bcb451a187c18099961c484eef8b
SHA1	99472c2d1918ea56c632734bc5c8a89ae6d2551c
SHA256	d988156066b7fd22de278fbc96759d2caea6552094ffeb2ddd9307806059c5e4
SHA512	a4d78de6bcc1e940c466c41c31ee100235b32fef4cb3e7815a9c62dfae1eb3e4588d2c9e8597152ad7754527643c59ea8b811277ac58e4134a3dbf1507fe97bf

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Edge Cloud Config\OperationConfig~RFe59456c.TMP

MD5	904e6e94a1d46374c8630cfd86cc729f
SHA1	e1d9c3f7813878acc6510d48d95b2bf48b2e1a0d
SHA256	8b2e057387e9714efef3580a36459acf56aab53c806cd7d7dbb6e17cef977ef9
SHA512	081e2a26252860ff8d8f7a9d0378ae56f0cc50574d13d2a121afdf74284963747ef874a4d73b1df7774cd8570972f4f513eefe0a0325fd088556d5b1ba946712

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Local State

MD5	b1288596386e72bf26904e2ae421b1f7
SHA1	be44b2ee12e50edfe2168ff7b9f2fda0364eca2f
SHA256	d0379da0db88d89b1d782e1054e02b3fdb7e1134d4689a588361f2427f172d77
SHA512	5200a254ba711730cb12df4011d9aeae946d00533f3022d9680605808b436c1e1b3b7944a561db608ec2097be9282e18fc1287066cb6f0ebfbf03131c51e8623

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State

MD5	13308bfc863b5d4b9814aba2d8d8a4f2
SHA1	3c40fd6f8e1de440f609039e01250b507e6ad149
SHA256	b7c9f46a2ea18aa7cd00bbdb2d9d8d2f4bdb3bb9918d7fb9418016995c3e56fe
SHA512	c3c9c75758d51eeeeadb863d7d00aa9e4fc7a6a0fe66961cc93796c27f3ebf077f089c33729b5884ccac80d1225ce7a4e06cc97be14eeea7c708b26bc6e9f78b

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_898879799\manifest.json

MD5	af3a9104ca46f35bb5f6123d89c25966
SHA1	1ffb1b0aa9f44bdbc57bdf4b98d26d3be0207ee8
SHA256	81bd82ac27612a58be30a72dd8956b13f883e32ffb54a58076bd6a42b8afaeea
SHA512	6a7a543fa2d1ead3574b4897d2fc714bb218c60a04a70a7e92ecfd2ea59d67028f91b6a2094313f606560087336c619093f1d38d66a3c63a1d1d235ca03d36d1

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	f5a3b29f9a977e23d6ca4eb728238f9f
SHA1	d2c5576fff1189eb66493b5b677d79a8ecead68d
SHA256	f4aa1676b1cc0e8c932821d57f7e6ec93246f48d7b840aca2d58ef9fac0ecd03
SHA512	6f692909efad02642f6c3a4b7cd10b21760c6fbfd3bae39d3b8a77b22460fcd5f6b0ab6e262b007e533c406a981968b3e0894697ca50be7f10bf557f1c1972f3

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1946387131\manifest.json

MD5 fbebd68ecaa98928909421f66909c054
SHA1 99d787d90f7ed2e5ad924f9c5668eb988b5a6c07
SHA256 ba5c9096d20a482aaa1aa9e5f98ad6127d3e97c2f21de84f7c78d9b8073c8e26
SHA512 749a3b2be47fe28399dc763888654a3e8d397e06e8d3c3af3965bb45846a1336e6ab4ca82c82c3df846b34a2afafa2156f2690e9bf347ab175408dc0171c61cc

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\AutoLaunchProtocolsComponent\1.0.0.10\protocols.json

MD5 1de85fec2dfcc28011a7c2aaab95eb5f
SHA1 80e8c954bfbe8f7ee5a2335c8d969ae033935dc3
SHA256 4fd800e7b1a5fb24b13fac2e31946d205012b7c28d8c61580b0669b2fa3517cc
SHA512 9c7dd37eb0c094b6aa05201e7c71a8f33b9db81284223bcfa595a44a6ac95d5a6820ab6f07b7aa8d26bf207454e94277bf35332e9c009ee63f083752b6b51750

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5 551baa462724351873ccd655a8b64ea3
SHA1 ce2be3c6d77008467bc61ac14822065cf2376630
SHA256 9ea5bbd4491542e3878ce1dc40d90744197996ad91a29e27be679d4bec62570d
SHA512 8de58d8e979531498751d7416c6b10671da1b048181a23081fc15e7aca69a96a93676b3bf01415c3b5f8d1973511e5823b0f11cacddfc3e5d01e82cefedff632

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1754071788\manifest.json

MD5 c3911ceb35539db42e5654bdd60ac956
SHA1 71be0751e5fc583b119730dbceb2c723f2389f6c
SHA256 31952875f8bb2e71f49231c95349945ffc0c1dd975f06309a0d138f002cfd23d
SHA512 d8b2c7c5b7105a6f0c4bc9c79c05b1202bc8deb90e60a037fec59429c04fc688a745ee1a0d06a8311466b4d14e2921dfb4476104432178c01df1e99deb48b331

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\WorkspacesNavigationComponent\1.0.0.5\nav_config.json

MD5 499d9e568b96e759959dc69635470211
SHA1 2462a315342e0c09fd6c5fbd7f1e7ff6914c17e6
SHA256 98252dc9f9e81167e893f2c32f08ee60e9a6c43fadb454400ed3bff3a68fbf0d
SHA512 3a5922697b5356fd29ccf8dcc2e5e0e8c1fd955046a5bacf11b8ac5b7c147625d31ade6ff17be86e79c2c613104b2d2aebb11557399084d422e304f287d8b905

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5 2a1939fc3b2926cf2b82fae71c5f6bee
SHA1 3f9d6974ce660bbc0c85f3d9741b734cfd466fac
SHA256 02092b017b3b45a2cf26673a6a2c3fa2b49ab211943cadade98b98777ee73afc
SHA512 cceb75873ca288bfcb71f5d74fec5ad8ca61807ec55369055f4fbd095fd904097c974102d3296db3a1aa949c6edc5abd1a7c320e53daaf947ee61c28f5659707

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences

MD5 d438435f08b484f2393747400dab5a8c
SHA1 0c9999dc5d33e9dc06014374ef52224dce6a0ff6
SHA256 1b1f2aa0c999511d21431827f50615df0d4977b4408dc0a816c08e8e36b5afab
SHA512 78e0a02baaa31d7bef2f773635d89fdc841680033def4098a584da22e7c755d57c0620df9b466f20ef19519e1288a3df9e43a03a02b2d646d8790af261b26480

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1929768173\manifest.json

MD5 a24a1941bbb8d90784f5ef76712002f5
SHA1 5c2b6323c7ed8913b5d0d65a4d21062c96df24eb
SHA256 2a7fe18a087d8e8be847d9569420b6e8907917ff6ca0fa42be15d4e3653c8747
SHA512 fd7dfec3d46b2af0bddb5aaeae79467507e0c29bab814007a39ea61231e76123659f18a453ed3feb25f16652a0c63c33545e2a0d419fafea89f563fca6a07ce2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Edge Data Protection Lists\2.0.0.0\office_endpoints_list.json

MD5 94406cdd51b55c0f006cfea05745effb
SHA1 a15dc50ca0fd54d6f54fbc6e0788f6dcfc876cc9
SHA256 8480f3d58faa017896ba8239f3395e3551325d7a6466497a9a69bf182647b25e
SHA512 d4e621f57454fea7049cffc9cc3adfb0d8016360912e6a580f6fe16677e7dd7aa2ee0671cb3c5092a9435708a817f497c3b2cc7aba237d32dbdaae82f10591c3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5 bf165c172af1f75083dd4c7e8915ad0e
SHA1 2eb27e18672fd0a1816ab00d00078a570eb62711
SHA256 30e8b5d48a130d6bf81847b89c208c7a087525e9b7d9a0a97bcf21598332b63b
SHA512 a58ad7ee2e18750242b9c5d53224218bef54ecd50e067170da12510559c455979fb0523044d4c23d5d5a523562165e471f95d939376df623bfdea9228ca25256

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_132762391\manifest.json

MD5	8ce95626b39ebc2401eee0b34c24fc7c
SHA1	f97a2fefe756f7a03e388e1333573b884730c2b0
SHA256	2d905d7b28b1afd313753d14f6a916a2e56ec4c1316bfa43046b09214ceb6090
SHA512	f04e4f695977918adf6e0603386b6f9c75a4a2202b0fe7215b642f3db491a1db398039cc28633b8e2541749403581622d28c1400f3f8fc66a3daab200e27266d

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	a15cd0a1e68c6b9c3945d3192091dc4a
SHA1	5162188f19a245162594501e5febb31a7626aeb4
SHA256	ce7879978d6dc1ebc353b93e509ab0dcd980bc78615af00080f3db1cb23e79d4
SHA512	a7ec103cf7c6fa801e1850205c4c06cadf96c21b1fd56db058a2980c472b1ff2f25c69a73f943de8dff815d69217995ad880e85ca7b8ced8cfa1c506315f7368

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_808274551\manifest.json

MD5	4055ba4ebd5546fb6306d6a3151a236a
SHA1	609a989f14f8ee9ed9bffbd6ddba3214fd0d0109
SHA256	cb929ae2d466e597ecc4f588ba22faf68f7cfc204b3986819c85ac608d6f82b5
SHA512	58d39f7ae0dafd067c6dba34c686506c1718112ad5af8a255eb9a7d6ec0edca318b557565f5914c5140eb9d1b6e2ffbb08c9d596f43e7a79fdb4ef95457bf29a

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	0ad641099b286eebf58a290b5bde86c0
SHA1	922d3e17ccc238f1bf276051af3ad5cdffb20397
SHA256	0c1b4dc8f72139abc5b2e25e5d0097c1d3529ae18001b1a64ff535e345378b32
SHA512	8661612608382058967a1f2ef25c7fbee41a3c2c748838346c044a48058ba081e84750e4a0de424903813499876fa7f69beba345d8ebc396340d830f1a7c81e0

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_184510105\LICENSE

MD5	ee002cb9e51bb8dfa89640a406a1090a
SHA1	49ee3ad535947d8821ffdeb67ffc9bc37d1ebbb2
SHA256	3dbd2c90050b652d63656481c3e5871c52261575292db77d4ea63419f187a55b
SHA512	d1fdcc436b8ca8c68d4dc7077f84f803a535bf2ce31d9eb5d0c466b62d6567b2c59974995060403ed757e92245db07e70c6bddbf1c3519fed300cc5b9bf9177c

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_184510105\manifest.json

MD5	44791df1f32899ba8f0fd1f235cd4711
SHA1	e5ab30e8b7610e92c81c99adb110e3a429fc3174
SHA256	8f8dae05e2623c591dc44dc5a91385b4355da91492a770f0ca99b509db6533e2
SHA512	729578ec403ba1410c5826f622d4db774d68e243112351f50cb5fcf231ebdf7fd9759bb5e2bd4a7bd6433c147ede44b78f4eef2eb08c456d4a430b55a149edd2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\TrustTokenKeyCommitments\2026.2.25.1\keys.json

MD5	48cb5a96ba70f0dfcca0a2185a9a0c79
SHA1	efdbdf44f7cfea2e3b34c6b2fc0dc37a1b5cef3e
SHA256	722047d2502aaec9c2c80b0f7d3b60b29d3f6aee27d656f489e4fbca9a7c1a00
SHA512	77eb7bc1bdea2b121b8d95fd8b5d14603d5e105dbf8c8e777b44109b1eb2ba65785ee3a094e18ffb591f81fe140ff83af1618d82680a5bb3a29144c58895dd2e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	3667a5e61a95ac2cf39c546762e1ead2
SHA1	021cfef6204b1473e294386a6c40e65eea92d231
SHA256	76878634fa32e0beb39c3a987dac8fdd35ed276fbeec087bb67a1f9485c2fb20
SHA512	7e93cd22f3e71a577600661f639c5237cfed67ca826e009cb220d53021cd2a4d78560e2871342905ee7cee1ad01f0188c5254db4df3dd85d72695506a0909cc5

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_668123467\manifest.json

MD5	2714a51ed8c2a891ad73b7488ab655b9
SHA1	9a8cc479aec8de1b4eb678e5d68b23b16a39dc99
SHA256	096e772e0f2e8c15e6dec9087ee0a1fb8b0c56b25061626aedc9e7e705adfc2e
SHA512	4811522c06ad6946626a9f4d12eb62a1d623825d18a1cd0ad7b628f4c059f37d299b5857abffd959e4ea53239412490539f5705b4aa6c6951d13c68e6d5b72ad

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	2912515e772da4827aeb26b89bcce599
SHA1	fe52983ff279b19e1eabd80893fcdf2332fe75b5
SHA256	f11d40368771778fee4d4fcdd04c8872c900acb26296fcc2ac6c10859a5edc8d
SHA512	088ea0d73cfac45d5561b898ebd2b9c486b4cef72dc6355fd1b0e8f3d926c482bb80c0cfef9c50f5d9ab27c1ef19a82a1e814deeb63680383bd4e76c512ee46f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old

MD5	e783f8b7294ae3f4278370ce959266eb
SHA1	900eb4dca9e1b063164a6a9418f2c150c7e3bcb5
SHA256	c7949adfcf00f1755d52773b20825c486a833741cadfa28269aab92f253d5e26
SHA512	25c98a487425a04066ed20ba86571014ceeaa0de01bfd212ae7e90044b035b37b30ec2049674b39352ad8d0a1e0263c82f2c9672f065585f5422183c7e2fa309

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old

MD5	7c9857bdd84c63814708606664963fd1
SHA1	327e4c87138729f28c15068f07e4e043ffa8c55e
SHA256	d95ccb373d74023494c9c6019b941cc866d1857eb6da107cf8d932c2f090730e
SHA512	a552036ec2a3c17ea6ad5d4f935626347e713e28b1c356ff1ab6b490da70334edef49c67cfc770810e1c4bea4f0dd5adf8f2ad90e8aeac400c39a3049ec3e270

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\48166f30-78f6-4da5-98a5-a0ff368b9888\index-dir\the-real-index

MD5	7a3853f4b41461220214a36eca94d806
SHA1	04719a7a22d5057d306d2f7f44bca8bb0cbda8db
SHA256	862c0abb5ec06624c79573af9655dff043a06df0b871b34a75c0df989a822e9e
SHA512	2ab02d1b99dd5be1cb5319eb48c2fe65f38ea47f600a2c012443fbceb60fa654928deed5182402c159ca95ad4936dc75337117dfcf9ecc4c852a4fa1a6736944

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\48166f30-78f6-4da5-98a5-a0ff368b9888\index-dir\the-real-index

MD5	e846fd961b45e2f92dc10013cbeed71a
SHA1	2e504f6f977ba679a940be604f160f120a4be155
SHA256	a76fa6b49dd261aa1526dc27d89e6bd3c8a15a0bc999496efe5672f957eb47bb
SHA512	80397cc2c1caf5bb8b317192084f666b014239d4686503d5e3ce9a570defa96997d49e63b67ca1d094912d16b322159f27429a70bcd0c61751d68739b5f7c3f2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences

MD5	2585eed5a338c51f2871522d7be55a07
SHA1	24356719640af917148c3fe37803ed2c3d183f34
SHA256	f8ccb4a4f2a8610668cf0b817c5c719f7b72bda39c00a1e9a0e737e45603228e
SHA512	6d201a039239d3d7128cf162c50316410fddbb60b153fda72f88b057f2ff17523fcd6fbb7bc76011de14513b632553afcc7860166b8773a83877457d4a2ea007

C:\Users\Admin\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\LocalState\DeviceSearchCache\AppCache1

MD5	8dd34eb698f037061e3a0ef9448c3cac
SHA1	2ab8e5383813f036c4c9a09d19efedfa833335c7
SHA256	97e7f85262d73304a930d45a5709e203f6880f21f265229e06e0d80fcc7f0a23
SHA512	c8e001a0cd8c7535c98a283a7cc01af89f241a995ea6bfd470b6e59f12ae5895a2e7d86d9d1866e524cd648d11559bbfad9e2465679190a207fc3170855d100c

memory/2664-1351-0x00000203C8120000-0x00000203C8220000-memory.dmp

memory/2664-1412-0x00000203FADC0000-0x00000203FAEC0000-memory.dmp

memory/2664-1413-0x00000204FC0B0000-0x00000204FC0D0000-memory.dmp

memory/2664-1416-0x00000203FB9E0000-0x00000203FBA00000-memory.dmp

C:\Users\Admin\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\AC\Microsoft\Internet Explorer\DOMStore\EQ7KSCOY\www.bing[1].xml

MD5	c72e0dc6655e2c0d51494f28ea0a667b
SHA1	543f8e9e780983d17a23ce2b1e4bdc61905b7e11
SHA256	3e8f1a2c2ca9fe9fc194cbfcf2d7b4b9313161622cb87ac6272442810774454e
SHA512	acb15025dea1020292cef5050f0bb2d0a8e6e32148f66e251d1c35fd67d898b180c2e47aa232478ff4173958b68d2ff6f9630d9dbe5c3b8fe8d7368bac871979

memory/2664-1486-0x00000204FE250000-0x00000204FE350000-memory.dmp

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Local State

MD5	07e095dd69f04cbfa4d8c11370ee31e0
SHA1	8c30f476970bbd9ee03a15a6fc053994166591c6
SHA256	eda5335dac9a4f2968f646a43d500ff45f2cc1bf83dee91c897ea25726494568
SHA512	8fe04558eaa8276f016a4c371f5220cddeace6e11e3db38f71c6622341ea78a39ef4b3602de4387360a0f1e95efd92a5c4ef59b0502db2b15217510fb474bb69

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1639303045\manifest.json

MD5	7ef3c71464d0fef472bc1d81fd363c62
SHA1	230e8ec0f849bf34d444c55ef548ba0c9c94d39b
SHA256	98821f71a1973ac61b45967ce0c121eb598ac6e95abaa23c912d2f33e4237d8c
SHA512	f74b96ec3b9569e360a02bfdd4fe237efad8ee2a5deaf46db891bcadd39dba22fd6d59a4e9aafe5511152625ce9f468519dadd53fc0c9b6c8826dc58cbe6cd7c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\CertificateRevocation\6498.2025.9.4\crl-set

MD5	d01869348d5a783f61f90cbb27b82a78
SHA1	d4eccc91435adaf01f8589cf7f3589cf65425de2
SHA256	6ddcaf50aaff98b960d067054ce2ce17872ac0719d02abbb7fe56b9eabc818f2
SHA512	7ad7f27d1f559d1f50f1f009518ccca5d6d01696cd70657ad94c9fe37db7bbe06e4afc13170bc5c065cf72d69a92c3df78f637b7faa2f968bb89aa154fe371da

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\index.txt

MD5	c5bae79b0ed4ff850c76ed881ae091cc
SHA1	cde4500f371fd1e11e7e396c50c5c23f5a4f24cc
SHA256	74cc55dcbee2ca89a722ef8193fd80a29f1a878055b2393c1a2b02ce9d02e7d8
SHA512	29eaa2c43572a62faa3da6f5f9f8e29aad5ba0c9387e51f0b3e33fccac1a7442705dc461d401eeae8147ef13c02ec3c665a7e67c111bdbc07aeb935d13809e20

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	e9afac9be384154e5d7c5a1d999a4e28
SHA1	3403fdc1732a4dbaa2c96cd4455f16cf761b2ae0
SHA256	657f92e7f14579a6a0113041b696909b9184515590665d5efc94268e1cc6613c
SHA512	de05316802f0151d449224e22927012f1f79518ec06c381eca9c9a959cc28240c1d651d7269970a0fc0f9ff82658d8588812210ed6cd81d63d46e7f8133f9be2

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1948944278\manifest.json

MD5	15b69964f6f79654cbf54953aad0513f
SHA1	013fb9737790b034195cdeddaa620049484c53a7
SHA256	1bdda4a8fc3e2b965fbb52c9b23a9a34871bc345abfb332a87ea878f4472efbd
SHA512	7eeee58e06bba59b1ef8744360352024160796l7b7953593abf6d9af42a55088ab37f45fdee394166344f0186c0cb7092f55ed201c213737bb5d5318e9f47908

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State

MD5	dcd9715aae4ac6403d23fccf17873cd6
SHA1	95cbc9adb16ec885c713ea05392c00fe402751dc
SHA256	d26092852880aa5e2a690375ca9827d03ea7c57d50fde170eab087d1946aef90
SHA512	d365f4c203f64b6fa11394b3f43e7b1a9c83d1eca69725bf43e6425e0719e465fec01323d98d1583caa9b91e36c6552b33d3acd0896efa3f1422f61771345ea6

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	ceda33a0c398a483fb886b92382ad689
SHA1	f2c9523b88f2989bd0b6875678e6c483d58f54f5
SHA256	08104c8e414eb7d0e2e87d438472c0882848d699162a0fbee7b85c2165afc0f4
SHA512	54a65808b0787245e8bc88fdd108cf27457d90b7e39283c9ac7a5f95e44bbacf446bbf003ed972ab5e816b657c96c22897938b2aa2986347a6a713364d767af3

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_2119453888\manifest.json

MD5	6573c73b7ed1c6cbcf46c46f495e2b7d
SHA1	73e3c97a7c2503dce8ffd2c7c03a632471ec5afe
SHA256	605fad4274a41aa5139f0339fd3f0ca2483c9507cad75df8269c01c0d75aeb4d
SHA512	e9bcf833d116faa47e992283af2aa3cefe7af97aca508cb1676794fe1562def41b43c254f7d8c06652b17bcb72854c0df1129c282148959420df606ee4f2e8a0

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Domain Actions\3.0.0.16\domain_actions.dll

MD5	4ef0ad12ffc81a3570d19817265b7197
SHA1	a70a993ad81ee36d5f719f2f046d30b397fb5191
SHA256	cd4e81ff9db4c6b086b70b09919b9426ca1f2c05ec43c477e9ce99156be66399
SHA512	c270a4d32d8f10eda440ce521cce4f29544b384577548ac0e43b869d726d9cd6d1b283020ade3bd8153b0fc5f6a93bb630b7139b2c627ad0b0e3fe78bf01f212

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	1431b112eccfb401e520f399f4f39e65
SHA1	c2cc050cb62a2deaca0e2afc952bc067243d54ca
SHA256	a765d48fb98484c2cc43590b056c323e702cf4ceeb8f094701b798794e0050ff
SHA512	1b726c4c7f81a50384659b6436a069a83f6b657801dbfc09accd503dd60938b02d286855b4f1372b4090b96d66b675fd022c548dc6941f65e76f9ab42f2b6646

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Autofill\4.0.1.32\edge_autofill_global_block_list.json

MD5 5d4464dabc1289c3a010e14c05b92c57
SHA1 d2d185faca1cd13a6d42dea68803a9941074707d
SHA256 7d3c45c8207ba69066516e51e10a2137bc4f1fce070a692e0c65225f9856e04c
SHA512 f93f4b58efc0127946ffa1b2950a1cf71da6f77a6ab4cf98ad8ada6a751d6261be4818ff8c64fe1f1d45467aa070e0823d15be36c8259c1044fb2d1289df9994

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Autofill\4.0.1.32\autofill_bypass_cache_forms.json

MD5 4b1a79b1996f03fb926a97912835c881
SHA1 ca43e23f7bbb4ff3839751f722df3c38ef7bd8a7
SHA256 f7510e38f81f8a84027304070205dd55127e3233fdf011411465ede67b5b5d92
SHA512 c2e07a1b311ab71d94c7b874d645fe1114fdccfe4468875d6b23318fbe327481a60b2782af105b7546b3c1e6c3a7ec67261b21a0587f914cc7bf77c55f1f568e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Autofill\4.0.1.32\v1FieldTypes.json

MD5 b1c140ef49f01eea089d3957da1a529f
SHA1 de64781f20aac98b4d2bbc497e3defa83b25aa8f
SHA256 611e7995ab7599a0c89f98d6c6152a42aaedf7449748109a465bb5b0badd0af2
SHA512 02ddfcbaf9eaff793f251bd983394cf473b1340182ac1f3217cb7258ddfbd2de066ab08af16b47a378644bcc1871ad6ed8c641f6a053802c90e77f648e4f4be8

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_649655351\manifest.json

MD5 7382260298fc06c135b7c7399e9acff9
SHA1 6a829f795a3b8be25200675e00abfa1908fdefdf
SHA256 7169d86e87f904218238cd293e043e20b7828afad9acd1ff2e5d64188530b9d7
SHA512 f0ce77f9f72fb6721bcfa9b03f77b0771e8217988183787c00dba4f9d9f19cdba252ddd656422336035f81939cb97c8b5dcb4f036a39280198c17cd04faaaed4

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5 ade3d0be058ef5519b72363eaa1f23fd
SHA1 34dfd6aa6f5109519fb6f0c6dfb277074be08991
SHA256 cdcf3616d88c5dd8a1230fe8b35a327d6b2674f225b98f45d1bffea690a95b9a
SHA512 433aba4c634d20e5b087587391fb81c0011049ddaf1a9903c6f9b1b8d73df55a1ec137118d7d5e5536227bca73007940aa7c2699f4d0820f4e049b1eb544d22f

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1761439032\manifest.json

MD5 a30b19bb414d78fff00fc7855d6ed5fd
SHA1 2a6408f2829e964c578751bf29ec4f702412c11e
SHA256 9811cd3e1fbf80feb6a52ad2141fc1096165a100c2d5846dd48f9ed612c6fc9f
SHA512 66b6db60e9e6f3059d1a47db14f05d35587aa2019bc06e6cf352dfbb237d9dfe6dce7cb21c9127320a7fdca5b9d3eb21e799abe6a926ae51b5f62cf646c30490

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\SafetyTips\3057\safety_tips.pb

MD5 bd6846ffa7f4cf897b5323e4a5dcd551
SHA1 a6596cdc8de199492791faa39ce6096cf39295cd
SHA256 854b7eb22303ec3c920966732bc29f58140a82e1101dffe2702252af0f185666
SHA512 aa19b278f7211ffaf16b14b59d509ce6b80708e2bb5af87d98848747de4cba13b6626135dd3ec7aabd51b4c2cfb46ed96800a520d2dae8af8105054b6cd40e0b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\SafetyTips\3057\typosquatting_list.pb

MD5 17c10dbe88d84b9309e6d151923ce116
SHA1 9ad2553c061ddcc07e6f66ce4f9e30290c056bdf
SHA256 3ad368c74c9bb5da4d4750866f16d361b0675a6b6dc4e06e2edd72488663450e
SHA512 ad8ed3797941c9cad21ae2af03b77ce06a23931d9c059fe880935e2b07c08f85fc628e39873fb352c07714b4e44328799b264f4adb3513975add4e6b67e4a63c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5 e161ee565127ce02ef8b1ab9ddda3a4e
SHA1 f10384cd92a5776d1200174761b7a722cd2c3379
SHA256 cc4492bdf1024232a88bf7c18cf5875777f0f51c7ae094d8875a97551ee54aa1
SHA512 d3194a133bc48f165da22949d4652afb8dd190e67b19c1cfc4474509b9f0a6c3a08b52f38f876532ffdd863e99f961e2fdf43f758df053b5cc14251a13c73894

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old

MD5 fa68c4bcc9fde3852a29da690455827c
SHA1 477d35154e1bbf4a9d67b0eccbd09b0bbfeb3437
SHA256 128134ecc78b90869a7aa0a7f835908823901cb81adf233d5089501c9e9cce4d
SHA512 a292c22ffae88c6401d96427ad8f268ffc172efca9c44c06129dd3af998a0313f8594e9dd0ec815b1ef836d4d2018eb87ddd88f484caca1851459b6f2bdb4e24

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\EADPData Component\4.0.4.1\data.txt

MD5	868418ae9c5d2cb6622da65faf86702b
SHA1	1d7923eeef3d6b584513d6db8880d26c52f3aa5f
SHA256	a2982a165c36b8f3624762f10749be694c8282f9b28c7e35965491794efe9591
SHA512	8935a3cd42725cbd2f331e97b25bc823867698f8128a628a05b03ed1ff040e083f17e790f278e66651b92ef6fb5cabfa4c0d8fc400e2ccf3f1a3866a2ed0571f

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1639174249\manifest.json

MD5	475ec9a4e5c674add6cf767f5c7d4169
SHA1	f013a3715c408287043b3d6e743ea81b529531e0
SHA256	06e5abe50177836b7b929390b260ce06a3d26ef79f0b4cb7873eb354ca26d6f9
SHA512	fcfad595263fc60d219f360774e6f6c9ebf7baecfe21483ef0cb40c02896e3d936fb1916b05e27422d91374896ae4addda7443a632ce158dab96eb3abd9ebb57

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	adebe8d031d45568f07d1c071afea790
SHA1	046bd48f45160046dd551354318bb11654007528
SHA256	328fb4630c44f243ddb00cce37214d15f48de987bebf6b89b06736a49d83e51c
SHA512	a46fb3a4560348934f18002fb9d15dedd3851bb7a507a0a209ba96c3f4c6c24e9239c908cfce6411a81944272eedabb2762a7007d806df5c78380150519f5804

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\MANIFEST-000001

MD5	692c7108cde443f3a6b6b3f142ef1eae
SHA1	3bf854f88c15019e602156169d06bb09565a0ca0
SHA256	b8fc4cff1e6fe3fe5c28d28b1d016f8be1af2e6d09a26ca52e63813e2159bbc7
SHA512	497598b24b64fa2e5931f490c0e1081d1339c9fda07c781b815f83534566e8af89f284074b5dbeb8e7e115a96f5032ae8833c88914350f826f11022e4eea4fb9

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\manifest.json

MD5	a4d9ab812da8b2906ff9d46f9ffc07c3
SHA1	48b428dc760bc008058e6df47a9f05f2f86b4abb
SHA256	68683970ce6d7de9a2043c34129106ae68af21a3b0a3c53cb59695640a7c1cbc
SHA512	5a2ba950ed85ee55bc1402d57d09ca8d54c0c2df5b43a402bb8bf3668920a40d584fa18d270376b046e23be00698bd1399ef6a0b695ee6c0b99fb454616b1cb6

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_1982923731\Sigma\Staging

MD5	0163de1b14421d4eee3757ff76fd81e4
SHA1	96c75c4fe1e3f33a367f45293bd1bd8bff1c06f4
SHA256	411a706def2e70f96a507208bf80bceb93e950c4c2d671cd1ddb4134ce54b2a9
SHA512	80114d59db8f3654dd6821589e5ad03daa923a35610a372756a8865b3e769621e32ef2aed92c2494de2b9fc06d9796b12f1e3bb75873ed794e8c9ae8a0d5e965

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\Entities

MD5	478a605d5578236f2d1ddc93c2f22456
SHA1	917f05453d497b3e3de684a905e141972c34a267
SHA256	f6e93c83d9e3cfdff064535647cee76fc85aa1c86fd22a93dcf3d2c377346d94
SHA512	26d75309976fac0bd03ffe7596209c50ead7518584dd9f27d12a86d80ecec0889bb58da1b8dc8cdb38fc6bfdca7928a54c5a15903c4b8d293633d4d58ec147b5

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Sigma\Other

MD5	7bb2f4076e4f47781b77d811b21ef1ff
SHA1	fc0feddf6f52841bbd780d21b8e0ddff74fd70ac
SHA256	c9ab8dbc87043c71dd649fc06bb006e7f62e81c973c37b125afb88e654e436f8
SHA512	28356614bc38576ecb37218f9f6f631bd9e55573206c3aa854b91956a33fc828c71f42c7dc7dc6aa86540dab8e345b8f88bf9c6eb56e49824f492854c193b27b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Sigma\Social

MD5	fbfc314bba2160b09a3376521c762772
SHA1	3566357486c5d466958334e813c90c0a97bfc985
SHA256	e520603e6fb543cd078b2a7dbd8ccfc175e9aecf71654fc19785927a014d3435
SHA512	e4383491ce5170d0daf4abee61484c62611dfc604549b537d0080f24bfb8cf379ec3efbfb6caf10e7c066ec06457fb077832d5f780d226f0a957f624e0ba9383

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Sigma\Fingerprinting

MD5	5330ccc991b45c6f2777d23c7d8afe8d
SHA1	d11187c035458fe1201608a91062962903de2e53
SHA256	ec0fcbf71d58e707aaf6ba8d3c0719972f26727febe03f8efbf570b9635faddf
SHA512	2db42b7a6b7f2170f6cad2a26a606ff6357cb8c707ba9947baab14dd7f566df04a274e46e36cee72c43ee87ebf4d455b4af3f6da973f29bdbefeb0304f1d6f93

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Sigma\Cryptomining

MD5	4ec1eda0e8a06238ff5bf88569964d59
SHA1	a2e78944fcac34d89385487ccbbfa4d8f078d612
SHA256	696e930706b5d391eb8778f73b0627ffc2be7f6c9a3e7659170d9d37fc4a97b5
SHA512	c9b1ed7b61f26d94d7f5eded2d42d40f3e4300eee2319fe28e04b25cdb6dd92daf67828bff453bf5fc8d7b6ceb58cab319fc0daac9b0050e27a89efe74d2734e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\Cryptomining

MD5	95aa820d67ec466eb3444a9458eb7e56
SHA1	f93e178ff40310e071e4d596f0aff0514666f787
SHA256	1e92781e88ee786bf6d1d5cb71d467a92fe7f281f2d1e548524bf119d7ddc700
SHA512	15281c334f013f0200ca2d6faaaec81dc5602058cf3522b805e21ca5f031cb4ca68606d353e6745bfb86f07fdd6ccc892942aee5ad7cf0f9f0798a4d7f497a47

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Sigma\Content

MD5	dee2a727844dd3cea088941e82722406
SHA1	24ebec9b92eeb6af83841ab02e858f415580f719
SHA256	d99df5936c57a50aebb7f0a3ca65fcc682f523ace93641fbcfb9b09cfb71c739
SHA512	e48edf5f6dcbbd615f42f1b3181b2998bd700508094466009a6a48193a48c3e30e6c4d71cc43aae81d18a88ad9fd7e28eb50a0a52ca6889a270001fecdb64dfb

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Sigma\Analytics

MD5	e018dfa2df54c80ffbfd02c6d2ff5430
SHA1	de3f876b05355c6024d76f1bc24a552e532e2a2a
SHA256	33d2b069ea874c12ec96242ca7eb539c1086d38ac6c2e4858c0efcd74fc632e5
SHA512	b6d7886b4094837b271d1aa1f72b8c521970527552186604bcb83e17f85fa4a22e658628f79eca7d164ace781555abaa07c423a380fe87006aaed77f53e37838

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Sigma\Advertising

MD5	6959a6835772c67f4e72105e4be259a2
SHA1	72d1fe9070a5c0eed55d989cbd961dbc5442796c
SHA256	868f3ed3f86f1e82a5041f0a7b382bdd720e411531df2dc680da34eb60580b75
SHA512	98085236a15e810642602e5dd475aa5a9532bb38917aef784e977bb398b3f9e39f7966370d39c1b554cf3e39858713e8b45bc27fbdb8a701b2a903e453a67591

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\Other

MD5	cd0395742b85e2b669eaec1d5f15b65b
SHA1	43c81d1c62fc7ff94f9364639c9a46a0747d122e
SHA256	2b4a47b82cbe70e34407c7df126a24007aff8b45d5716db384d27cc1f3b30707
SHA512	4df2ce734e2f7bc5f02bb7845ea801b57dcf649565dd94b1b71f578b453ba0a17c61ccee73e7cff8f23cdd6aa37e55be5cb15f4767ff88a9a06de3623604fbf0

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\Social

MD5	1d06d58fe9131c14ba5ba5ff740b020f
SHA1	e6ed812e23e201b20170e928686a5d612165df85
SHA256	4955c3e7f56641a4ae0ce9c79b4ceee4b21733b0f6dedc980bf8d822a792eba2
SHA512	2854c73c6ef4d271d0e992113732ad65e406d6310711551952b4d451e2c577a2c3dcb06052e3ab30003b01619a39e87e5dd28d54f459f94efe879d1a79039b8f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\Fingerprinting

MD5	3d90e5235a4bee8f1dccfc2aecf7c585
SHA1	5beb333084b3af33e7fbd8c83326e18650a87f85
SHA256	c7d2b05ff6e790af78b0f1f341219fdb554dc5e14fbf3e3981819fccdd1ddfed
SHA512	c81af723cadaa57f638b9dbc60aca5d2600cebb8282d78a7b86edc6b473bd3a1768c8fde1b11d50b6b967b2866495655de09577973778038434bf4b513ba74a7

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\Content

MD5	26c006f350f70dbc8c18098b773c3d4c
SHA1	eb015f7010dd74c874675d0599e634027363b7b4
SHA256	7869993fcb93b302598643be96c6ab94c4f3be47c9fc344959773c754291376e
SHA512	0f56d119a5f89689d0e45a6163133048aa95255447c4156d4fb2565f45c32dbb95adc39666a833d2127ce57f3f4198ce45d2a174955ec088bcdd2f74f59b3f6b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\Analytics

MD5	db9a3dbc4820c8d84a0a569be1234dc0
SHA1	78fe9b49b800627cd2eb458cbe0251591a2a693a
SHA256	163a5318312b814104d244a4b37b676a02f827068820aa60fc069e6346cb2b75
SHA512	a6735713a801d28e644b31f34335e29d55a46d4b263e923cbec9b57fd18f8b0cecf9b78fab578065207080faa5e81156d04c8fbedb436b718893b6d17123742c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\Advertising

MD5	3495430eefd1e96e8bd95b67ccab0f91
SHA1	54129d2d72e062ad36a66922331818e81bd34df3
SHA256	5989ccf9a58e4ffd47c2422bd8dfcb3ea4e1d412fbdec2291385a9955af9eace
SHA512	9197537719b70837ce997cd2b168c6bf6fe877811f81459a0c0f1363b7179960594761df147c85034c628b8e9a3463084ac26fb8bcc3fbc765089adfeea56f6b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Sigma\LICENSE

MD5	5b7baf861a48c045d997992424b5877b
SHA1	2b2bd9a13afe49748abf39faf9eb29ed658f066e
SHA256	44071e0fcffb9a9a32e8fa7010bb18dbc41afd0b176f81bf700b15b638a88a51
SHA512	4820b41aa5ff4d934a583e1f0b93b1512631102bb2dfdb74792a2f0dcf9907da7680c02a5ddd2492a1e6d58cdada3453d9e38bb8deab6ce831ff36a7f8de016c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Sigma\Entities

MD5	751e7cc660220e7464935a9b90643274
SHA1	05a725af45c74a9e129839b2fa7acca5d83066d8
SHA256	0f305323c627cf0c790831c7e0bc38455b7a99983c4ab5bd9d2d9567766c3499
SHA512	bc879a9bed224b6abdaed2581f948fcad53361b17dc76d5b5df10607ac893db2f39bc5ce5fbbe86e6392ae66f29fc93ac1079fd2d029b9338697b004325c4b36

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\TransparentAdvertisers

MD5	57d5a3548911886de2f3bd3172e808ed
SHA1	ca932af3b25f245ce931fbc6cf10299e5fbe35a7
SHA256	d2cd0bef5f45daf490c53e705d6f67dfe12390c72a00efa6f5117432bd8edb8c
SHA512	933194509d305b2a60b38c149ba1d74e142ef15647242b287844d263006d33ffa38b6ea263c89cb821a9277d41f0cfda95a0eda830f3a5ef8df5ba80d3bbc818

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\LICENSE

MD5	d32239bcb673463ab874e80d47fae504
SHA1	8624bcdae55baeef00cd11d5dfcfa60f68710a02
SHA256	8ceb4b9ee5adedde47b31e975c1d90c73ad27b6b165a1dcd80c7c545eb65b903
SHA512	7633623b66b5e686bb94dd96a7cdb5a7e5ee00e87004fab416a5610d59c62badaf512a2e26e34e2455b7ed6b76690d2cd47464836d7d85d78b51d50f7e933d5c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Trust Protection Lists\1.0.0.34\Mu\CompatExceptions

MD5	108de320dc5348d3b6af1f06a4374407
SHA1	90aa226d3c9d50cf4435ecdd2b8b0086d8edeb8b
SHA256	5b462316a51c918d0bae95959bf827cb9c72bbd84ffb0e43b750aa91fbf3ba53
SHA512	70f30c45e20b7cddd0cba6476af9338975cec8e40b8b19603af5fa859a34c6eb2138957daaa263633fe65213e2186402d05d9d29ad53e8f311335555116314c2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	07829e7fd81c7ac7cccb4c5f3ed91c4c
SHA1	8449540bd39662b82389760cf5b8400c7d7426d9
SHA256	9d312b58a575cc4308f30975ed29ab15911999e7990b2cf861813998c901bb7b
SHA512	30280226ef2f1ce4898cd635bf5b83c4e2935b2152f44ffe6472dbb1f4d3f26123f5a0598f1686fde7181748926e5cf5147d0df15cf91e01a6cfdd52a55edd60

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_981733079\manifest.json

MD5	50558b365ad40a8213fb79e84d42ffa3
SHA1	497d5ad94af7cecd6457fbd5723b6635ccd67c6b
SHA256	8ee8a2fb7167ad2dcf2dd6f56074509dedd711b1825dcba2629af48c89eeebbe
SHA512	165a117c8f8247263c3328def089e5bc159895e1d4375bd3df93df8f9208c571dc7e3fb98389fa36952c6f3d8f3add4fe5c97b22bddc01ef7c4ac37477cc608a

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\PKIMetadata\28.0.0.1\ct_config.pb

MD5	b83d9c00b73ffd5b6945370fee4bdb26
SHA1	dc5e7ab71b439abe18cde2c4309ef4452220d0de
SHA256	b42799f862739fed511f2527d4796690e23014ecdc02489074df4c44c60f272d
SHA512	fff0baa29fcb0253be4f916dd6fde7efdf6b20c49c851e4ff6a027b055a7a48a8dbb74827d55b525c3b1e7e53e27f84e2563f8cb5b7092911d651f4cdbb967ba

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\PKIMetadata\28.0.0.1\crs.pb

MD5	3ef7a7be0ecfef355a5d5d6e77ebddfd
SHA1	5c6e47340a710019b97b1fd58624f714420b79f1
SHA256	576d77d3085ff9156298e60dee868364cabab7911edf6f9a4d3ad5f351d5059f
SHA512	812f5a4e1f572b7a012add71bc210281fd362f48ba5a863b2e5a7d7b6405dd08632dc39ce650a0d032f926d1e41acd8f1c84d5b60552ad9ac98ad6d2abb7f265

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\PKIMetadata\28.0.0.1\kp_pinslist.pb

MD5	269f13e71015d2f9da1fc0e0e22b27c7
SHA1	67b35f4044517ec8b169d27d354a61e2f095895a
SHA256	1b9ee7a3aec303937fd884335b23591b55e0d5901d1ee25aa25800d1c202a24b
SHA512	039d3f870a4475ded4f972891059a4ebc467588f349d0310e47c9c975c793fbfe4179dc64f5c2616914aa97bcd5e83d6333f5de113f5c56c2fc3f2b7bb012dec

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	8de96579713b6da87317db9f8bcf503c
SHA1	0ce017831e85aa224c298f62ba5e8dc35cb81929
SHA256	3cab7a9883ba87bd55bedec9f2c23503a65e8939eb0d2e1e19d547b3d19b253a
SHA512	2d07cf6b8bc09eec47979c429da1c83de9072c76c4039501cb24e76ae26bac3d445925ac3bc26d126003eb68df7dab1eaa9ff99f6b26b89bd2b2edb525a2797d

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping752_14636026\manifest.json

MD5	811f0436837c701dc1cea3d6292b3922
SHA1	4e51a3e9f5cbf8c9c96985dabe8ffc2de28dae87
SHA256	dbfb38a16e33a39c35ac50bd81782e4608be14954f1df69ac8272c0b9ce87a5d
SHA512	21e7bf2f8333b2900bcbcb871ede14684073249597d105095dc7d3f101e7ccc326068732f11d4a167365f245a3f2205793f520c7666d7f948e70919b40b43d35

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Well Known Domains\1.2.0.0\well_known_domains.dll

MD5	f5f5b37fd514776f455864502c852773
SHA1	8d5ed434173fd77feb33cb6cb0fad5e2388d97c6
SHA256	2778063e5ded354d852004e80492edb3a0f731b838bb27ba3a233bc937592f6e
SHA512	b0931f1cae171190e6ec8880f4d560cc7b3d5bffe1db11525bd133eaf51e2e0b3c920ea194d6c7577f95e7b4b4380f7845c82eb2898ad1f5c35d4550f93a14b6

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\component_crx_cache\metadata.json

MD5	a5e9a4e1b2f6ed8cda8ee08ecdb41c01
SHA1	1ee7bf3814132d137b6701704a892d11fc030a74
SHA256	21637df4d8a7c3a2621ad7bee5e532a8e737f24e66790de0852c5e24970f371a
SHA512	e3d90e17c61d3de58dd7e2c925eff49018b20e850733afbf4e9c3c513a299b6963e0519ddbb9bf1dda7f95a6512a06f6fc781ca9d8092a43d547ffe797812b6d