Recorded Future® Sandbox

Malware Analysis Report

2026-02-15 05:01

Sample ID	260215-fcn44sbw8a
Target	WhatsApp Installer (4).exe
SHA256	f71f11a180a372dafd8a07608f796ad71e90427ed9f404a71a4d961def979b59
Tags	adware defense_evasion discovery spyware

score

8/10

Table of Contents

Part 1. Analysis Overview

score

8/10

SHA256
f71f11a180a372dafd8a07608f796ad71e90427ed9f404a71a4d961def979b59

Threat Level: Likely malicious

The file WhatsApp Installer (4).exe was found to be: Likely malicious.

Malicious Activity Summary

adware defense_evasion discovery spyware

- **Downloads MZ/PE file**
- **Executes dropped EXE**
- **Subvert Trust Controls: Mark-of-the-Web Bypass**
- **Drops file in Windows directory**
- **Untrusted Codesign Signers**
- **Enumerates physical storage devices**
- **System Time Discovery**
- **Browser Information Discovery**
- **NTFS ADS**
- **Modifies data under HKEY_USERS**
- **Suspicious use of SetWindowsHookEx**
- **Suspicious use of SendNotifyMessage**
- **Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary**
- **Checks processor information in registry**
- **Modifies Internet Explorer settings**
- **Suspicious use of WriteProcessMemory**
- **Suspicious behavior: AddClipboardFormatListener**
- **Suspicious behavior: EnumeratesProcesses**
- **Enumerates system info in registry**
- **Suspicious use of AdjustPrivilegeToken**
- **Modifies registry class**
- **Suspicious behavior: GetForegroundWindowSpam**
- **Suspicious use of FindShellTrayWindow**

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Reconnaissance TA0043			
Resource Development TA0042			
Initial Access TA0001			
Execution TA0002			
Persistence TA0003			
Privilege Escalation TA0004			
Defense Evasion **TA0005**	Modify Registry T1112	Subvert Trust Controls T1553	
		SIP and Trust Prov… T1553.003	
Credential Access TA0006			
Discovery **TA0007**	Browser Information Disco… T1217	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 (4).exe	2026-02-15 04:43

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 (4).exe	f71f11a180a372dafd8a07608f796ad71e90427ed9f404a71a4d961def979b59	1.1MB

Submitted	Reported	Platform	Max time kernel	Max time network
2026-02-15 04:43	2026-02-15 04:59	win11-20260130-en	900s	902s

4. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (4).exe"
```

4. 3. Signatures

Downloads MZ/PE file

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

Executes dropped EXE

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\Downloads\WhatsApp Installer.exe	N/A
N/A	N/A	C:\Users\Admin\Downloads\WhatsApp Installer.exe	N/A

Drops file in Windows directory

Description	Indicator	Process	Target
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-shared-components\fr\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\manifest.webapp.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\Mini-Wallet\miniwallet.bundle.js.LICENSE.txt	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-ec\es\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-ec\ko\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-ec\ru\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-notification\de\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-tokenized-card\en-GB\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\wallet\wallet-checkout\merchant-site-info.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-notification\ar\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-hub\ru\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-tokenized-card\zh-Hant\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_392829847\edge_driver.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-notification-shared\ru\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\Wallet-BuyNow\wallet-buynow.html	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_392588867\Filtering Rules-CA	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Description	Indicator	Process	Target
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_392588867\Part-ES	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-ec\de\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-ec\pt-BR\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-hub\de\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-hub\sv\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-notification\fr\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-notification-shared\el\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\hub-signature.txt	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-hub\zh-Hant\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-mobile-hub\sv\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\wallet\README.md	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\wallet\wallet-eligibile-aad-users.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-notification-shared\zh-Hant\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-shared-components\th\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\wallet\wallet-stable.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_98101764\typosquatting_list.pb	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-shared-components\pt-BR\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-tokenized-card\de\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\wallet-crypto.html	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-ec\cs\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-mobile-hub\nl\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-shared-components\zh-Hant\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_392588867\adblock_snippet.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\load-hub-i18n.bundle.js	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_BeginUnzipping5772_580354290\json\i18n-notification-shared\de\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_392829847\edge_tracking_page_validator.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-ec\ja\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-hub\nl\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-notification-shared\fr-CA\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-notification-shared\sv\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\wallet\wallet-tokenization-config.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-ec\en-GB\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Description	Indicator	Process	Target
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-hub\fi\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-mobile-hub\ru\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-notification-shared\ja\strings.json	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_BeginUnzipping5772_580354290\json\i18n-shared-components\da\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-mobile-hub\pt-PT\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_1435100934\LICENSE	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_1435100934_metadata\verified_contents.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_1435100934_platform_specific\win_x64\widevinecdm.dll.sig	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-ec\nl\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-mobile-hub\it\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\wallet\wallet-checkout\checkoutdata.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\Notification\notification_fast.html	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-mobile-hub\id\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-shared-components\sv\strings.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Subvert Trust Controls: Mark-of-the-Web Bypass

defense_evasion

Description	Indicator	Process	Target
File opened for modification	C:\Users\Admin\Downloads\WhatsApp Installer.exe:Zone.Identifier	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
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.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\Google\Chrome\Application\chrome.exe	N/A

Checks processor information in registry

Description	Indicator	Process	Target
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
Key opened	\REGISTRY\MACHINE\Hardware\Description\System\CentralProcessor\0	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\~MHz	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A

Enumerates system info in registry

Description	Indicator	Process	Target
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemManufacturer	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemFamily	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemSKU	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.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\SystemManufacturer	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
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:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key opened	\REGISTRY\MACHINE\Hardware\Description\System\BIOS	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemManufacturer	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemProductName	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS\SystemManufacturer	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
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:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\BIOS	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Modifies Internet Explorer settings

adware spyware

Description	Indicator	Process	Target
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\Main\OperationalData = "9"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersionHigh = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\GPU\SubSysId = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\CVListDomainAttributeSet = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\TabbedBrowsing\NTPMigrationVer = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\StaleCompatCache = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\VersionManager	C:\Program Files\Internet Explorer\iexplore.e	N/A

Description	Indicator	Process	Target
		xe	
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\Main\OperationalData = "8"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\Main	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\GPU\SoftwareFallback = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersionLow = "395196024"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\VersionManager\FirstCheckForUpdateLowDateTime = "94823343"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\Protected - It is a violation of Windows Policy to modify. See aka.ms/browserpolicy	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\CVListXMLVersionLow = "395196024"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\GPU\DeviceId = "140"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\TabbedBrowsing	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\CVListXMLVersionHigh = "268435456"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\GPU	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersionHigh = "268435456"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\VersionManager\FirstCheckForUpdateHighDateTime = "31235738"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\Main\CompatibilityFlags = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersionLow = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\Protected - It is a violation of Windows Policy to modify. See aka.ms/browserpolicy\HomepagesUpgradeVersion = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\Main\DisableFirstRunCustomize = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\GPU\\VendorId = "5140"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\GPU\Revision = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\Main\OperationalData = "13"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\StaleCompatCache = "0"	C:\Program Files\Internet Explorer\iexplore.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
Key created	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
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 = "134156042650069823"	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Modifies registry class

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\Local Settings	C:\Windows\system32\OpenWith.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\Instance\	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\Instance\	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\Instance\	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key created	\REGISTRY\MACHINE\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-600123060-2148212387-2211176695-1000\{6566DE05-1E40-484D-9138-EFB5C72ACB9E}	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key created	\REGISTRY\MACHINE\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-600123060-2148212387-2211176695-1000\{5A9D6ACE-A263-41CC-8B6B-35E971042594}	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-620072444-2846605723-1118207114-1642104096-81213792-2370344205-2712285428	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-620072444-2846605723-1118207114-1642104096-81213792-2370344205-2712285428\Moniker = "cr.sb.odm3E4D1A088C1F6D498C84F3C86DE73CE49F82A104"	C:\Program Files\Google\Chrome\Application\chrome.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\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-1-5-21-600123060-2148212387-2211176695-1000\{9876FF74-18CE-4564-99BC-0813F5C11A4D}	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\Instance\	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-620072444-2846605723-1118207114-1642104096-81213792-2370344205-2712285428\DisplayName = "Chrome Sandbox"	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-620072444-2846605723-1118207114-1642104096-81213792-2370344205-2712285428\Children	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\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-1-5-21-600123060-2148212387-2211176695-1000\{8CED5844-B2A6-4E6B-9A5E-6013BCA83923}	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Description	Indicator	Process	Target
Key created	\REGISTRY\MACHINE\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-600123060-2148212387-2211176695-1000\{1AF3D612-E441-4466-B73E-07627F125E51}	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.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\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-1-5-21-600123060-2148212387-2211176695-1000\{1D2ABB90-238D-4D47-8E5D-3580A7045A20}	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-600123060-2148212387-2211176695-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\Instance\	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

NTFS ADS

Description	Indicator	Process	Target
File opened for modification	C:\Users\Admin\Downloads\WhatsApp Installer.exe:Zone.Identifier	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Suspicious behavior: AddClipboardFormatListener

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.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
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.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\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.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\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Suspicious behavior: GetForegroundWindowSpam

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.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
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:\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\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.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
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Suspicious use of AdjustPrivilegeToken

Description	Indicator	Process	Target
Token: SeDebugPrivilege	N/A	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (4).exe	N/A
Token: SeDebugPrivilege	N/A	C:\Users\Admin\Downloads\WhatsApp Installer.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Users\Admin\Downloads\WhatsApp Installer.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Description	Indicator	Process	Target
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeCreatePagefilePrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
Token: SeShutdownPrivilege	N/A	C:\Program Files\Google\Chrome\Application\chrome.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:\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

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
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
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
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\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A

Suspicious use of SendNotifyMessage

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

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
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.exe	N/A
N/A	N/A	C:\Program Files\Google\Chrome\Application\chrome.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
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
N/A	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.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
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 SetWindowsHookEx

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	N/A
N/A	N/A	C:\Program Files\VideoLAN\VLC\vlc.exe	N/A
N/A	N/A	C:\Windows\system32\OpenWith.exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 4908 wrote to memory of 5772	N/A	C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (4).exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 1432	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 1916	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 6052	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 6052	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 4192	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 4192	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 4192	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 3348	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 3348	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 3348	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 3016	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 3016	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 3016	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2008	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2008	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2008	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2172	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5876	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2172	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5876	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5356	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 5772 wrote to memory of 4792	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 4792 wrote to memory of 5516	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 5772 wrote to memory of 5444	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2536	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 436	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 5772 wrote to memory of 5444	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2536	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2536	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5212	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5212	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 3936	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Users\Admin\Downloads\WhatsApp Installer.exe
PID 5772 wrote to memory of 3600	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5840	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 1252	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3936 wrote to memory of 1868	N/A	C:\Users\Admin\Downloads\WhatsApp Installer.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5916	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5916	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5916	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5588	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5588	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5588	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 4576	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Users\Admin\Downloads\WhatsApp Installer.exe
PID 4576 wrote to memory of 3728	N/A	C:\Users\Admin\Downloads\WhatsApp Installer.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 4384	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 4384	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 4384	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 988	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 988	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 988	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 1136	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 1136	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5156	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5156	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 3476	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 3476	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2228	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 4236	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 4236	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 5772 wrote to memory of 5924	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 5924	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2988	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5772 wrote to memory of 2988	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

4. 4. Processes

C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (4).exe

```
"C:\Users\Admin\AppData\Local\Temp\WhatsApp Installer (4).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,0x368,0x7ffbeb97c188,0x7ffbeb97c194,0x7ffbeb97c1a0
```

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=1688,i,11484801943004432429,4933022937738288131,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=2212 /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=SAAAAAAAAADgAAAIAAAAAAAAAAAAAGAAAQAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --always-read-main-dll --metrics-shmem-handle=1548,i,9164255192272444901,10925404196937703850,262144 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=2180 /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=2452,i,15651582305640271738,17690908388063287572,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=2464 /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=3448,i,9564642118115042875,15417954607178477034,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=3524 /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=3452,i,18280579277915972131,7895962125702955055,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=3528 /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 --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=7 --always-read-main-dll --metrics-shmem-handle=4904,i,4878946011041507045,17384836361159956751,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=4888 /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=4920,i,9483805049748490191,8200417048376340512,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=3856 /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=4908,i,6484903325700386800,17234102198156767344,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=4892 /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=5880,i,5142261805238693054,11948155860065675759,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=5896 /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=5880,i,5142261805238693054,11948155860065675759,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=5896 /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=5972,i,1961190950887699583,6107252508782777041,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=5940 /prefetch:14
```

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

```
cookie_exporter.exe --cookie-json=1128
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"  --no-startup-window --win-session-start
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_collections.mojom.CollectionsDataManager --lang=en-US --service-sandbox-type=collections --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6340,i,7530715099206979353,6155494328378382359,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=6328 /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=13 --always-read-main-dll --metrics-shmem-handle=6376,i,2819939861997542398,12332087576996353391,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=6252 /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=quarantine.mojom.Quarantine --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6488,i,1495682204451747 72,10673448546985483460,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=6504 /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.UtilReadIcon --lang=en-US --service-sandbox-type=icon_reader --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=6936,i,13468152169608179737,10266013059360857251,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=6940 /prefetch:14
```

C:\Users\Admin\Downloads\WhatsApp Installer.exe

```
"C:\Users\Admin\Downloads\WhatsApp Installer.exe"
```

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=4888,i,17996582048144426120,14903666402002403709,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=4936 /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=3428,i,15028264976613616133,112469886712788468,524288 --field-trial-handle=2184,i,10786653303059596 94,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=7444 /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=4924,i,12638295005141454621,4922294169513687099,524288 --field-trial-handle=2184,i,10786653303059596 94,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=5020 /prefetch:14
```

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=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=19 --always-read-main-dll --metrics-shmem-handle=3428,i,2344499492478313522,13975533493390284862,2097152 --field-trial-handle=2184,i,10786653303059596 94,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=5016 /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 --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=20 --always-read-main-dll --metrics-shmem-handle=7836,i,4153724427208295453,15893054698171209513,2097152 --field-trial-handle=2184,i,10786653303059596 94,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=7788 /prefetch:1
```

C:\Users\Admin\Downloads\WhatsApp Installer.exe

```
"C:\Users\Admin\Downloads\WhatsApp Installer.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=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=21 --always-read-main-dll --metrics-shmem-handle=6336,i,3441202818038396528,16631891924582440073,2097152 --field-trial-handle=2184,i,10786653303059596 94,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=6264 /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 --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=22 --always-read-main-dll --metrics-shmem-handle=7916,i,99866586888674087,7140993114057267272,2097152 --field-trial-handle=2184,i,10786653303059596 94,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=7880 /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=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=8020,i,10521251812846513363,3508139268589625553,524288 --field-trial-handle=2184,i,10786653303059596 94,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=6620 /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=7488,i,10925036180494311182,3416721912578430111,524288 --field-trial-handle=2184,i,10786653303059596 94,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=7564 /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,17606571838910825678,10157436430447081161,524288 --field-trial-handle=2184,i,10786653303059596 94,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=5336 /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=SAAAAAAAAADoAAAIAAAAAAAAAAAAAGAAAQAAAAAAACEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAABAAAAAAAAACAAAAAAAAAIAAAAAAAAAA== --always-read-main-dll --metrics-shmem-handle=6020,i,17640572264923478396,3314984786266385119,262144 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=3508 /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=5532,i,16818795043363219390,8819545539349948644,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=7604 /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=6108,i,16037020812975851530,14268655338233094869,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=7996 /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=6116,i,15342390501511279136,8709782555349396740,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=6104 /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=3088,i,4385244756475397779,1818699046119936548,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=6316 /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=7628,i,14697151659773216275,6150013443820584406,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=5360 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --instant-process --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=32 --always-read-main-dll --metrics-shmem-handle=5356,i,6053559917564744927,1132507799987017649,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=5352 /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=edge_xpay_wallet.mojom.EdgeXPayWalletService --lang=en-US --service-sandbox-type=utility --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=7536,i,3062332000791272979,1977034868250707242,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=6296 /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=868,i,7708949178576733621,17739027352076675151,524288 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=7532 /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=37 --always-read-main-dll --metrics-shmem-handle=7488,i,15262401433528466632,820492659986274241,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=7504 /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 --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=38 --always-read-main-dll --metrics-shmem-handle=3856,i,14721057670821039624,6602267172822851442,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=7324 /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 --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=39 --always-read-main-dll --metrics-shmem-handle=8484,i,730794043933315670,12381784688067628908,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=8436 /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 --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=40 --always-read-main-dll --metrics-shmem-handle=5064,i,18398647624844223855,1696168609858633817,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=4920 /prefetch:1
```

C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE

```
"C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\Admin\Desktop\ConnectTest.docx" /o ""
```

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=41 --always-read-main-dll --metrics-shmem-handle=8312,i,829241810721704801,16520405185245631821,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=8820 /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 --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=42 --always-read-main-dll --metrics-shmem-handle=6792,i,1791775840095076493 3,16470576649205084417,2097152 --field-trial-handle=2184,i,1078665330305959694,10746478045198118123,262144 --variations-seed-version --mojo-platform-channel-handle=5104 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window
```

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=0x240,0x244,0x248,0x23c,0x2b4,0x7ffbeb97c188,0x7ffbeb97c194,0x7ffbeb97c1a0
```

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=1768,i,11278284328095604232,15026592233549048045,524288 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=2800 /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=SAAAAAAAAADgAAAIAAAAAAAAAAAAGAAAQAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --always-read-main-dll --metrics-shmem-handle=1624,i,12316576643561179101,8913453736726630077,262144 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=2704 /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 --no-pre-read-main-dll --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=2124,i,12392696426217286700,11226685068070397683,524288 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=2820 /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\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=4424,i,18434588806159284503,12580967647315513540,524288 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=4440 /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=4424,i,18434588806159284503,12580967647315513540,524288 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=4440 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe"
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Users\Admin\AppData\Local\Google\Chrome\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Crashpad" "--metrics-dir=C:\Users\Admin\AppData\Local\Google\Chrome\User Data" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=140.0.7339.81 --initial-client-data=0xfc,0x100,0x104,0xe8,0x108,0x7ffbf20cc728,0x7ffbf20cc734,0x7ffbf20cc740
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.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 --subproc-heap-profiling --metrics-shmem-handle=1508,i,12673219083340713250,309914812065222510,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=2120 /prefetch:11
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --no-pre-read-main-dll --force-high-res-timeticks=disabled --subproc-heap-profiling --gpu-preferences=SAAAAAAAAADgAAAIAAAAAAAAAAAAAGAAAQAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --metrics-shmem-handle=1640,i,19805629614374036 82,5200792874289489355,262144 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=2088 /prefetch:2
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --subproc-heap-profiling --metrics-shmem-handle=2408,i,2169457243223706513,1801756546223372323,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=2420 /prefetch:13
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --subproc-heap-profiling --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=6 --metrics-shmem-handle=3272,i,14277489735200355926,4099295398916210685,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=3280 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --subproc-heap-profiling --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 --metrics-shmem-handle=3304,i,16860640954569339712,6712458346223261817,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=3324 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\140.0.7339.81\elevation_service.exe

```
"C:\Program Files\Google\Chrome\Application\140.0.7339.81\elevation_service.exe"
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --extension-process --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --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=7 --metrics-shmem-handle=4236,i,3819528034007367558,15057500620740296874,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=4248 /prefetch:9
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --subproc-heap-profiling --disable-gpu-compositing --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=8 --metrics-shmem-handle=4568,i,449382953073979859,6531311251848250526,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=4716 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --subproc-heap-profiling --metrics-shmem-handle=4884,i,11101256869422805659,14551705498833844515,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=4216 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --subproc-heap-profiling --metrics-shmem-handle=4080,i,10621431187098345449,14837974107462544733,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=4528 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.ProcessorMetrics --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --subproc-heap-profiling --metrics-shmem-handle=5392,i,16330590833622904320,4389019133591824575,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=5128 /prefetch:14
```

C:\Windows\system32\svchost.exe

```
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s NgcSvc
```

C:\Windows\system32\svchost.exe

```
C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s NgcCtnrSvc
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --subproc-heap-profiling --disable-gpu-compositing --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=12 --metrics-shmem-handle=5400,i,11847071430370034404,7818544484186372181,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=5408 /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=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=4740,i,14288030812064306006,17639815590948638045,524288 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=4748 /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=4736,i,13634804041731151159,7077454665708145485,524288 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=4780 /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=4500,i,16341869004695292177,2325153138838114307,524288 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=4816 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --subproc-heap-profiling --disable-gpu-compositing --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=13 --metrics-shmem-handle=5776,i,10685588458716892643,34368706678975723,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=3476 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --subproc-heap-profiling --disable-gpu-compositing --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=14 --metrics-shmem-handle=5740,i,13431993407158790567,7123121275327120519,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=3520 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --subproc-heap-profiling --disable-gpu-compositing --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=15 --metrics-shmem-handle=3444,i,9843316226160718324,15612483190865844131,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=3848 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.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 --subproc-heap-profiling --metrics-shmem-handle=5768,i,4633965160101209787,11265368291579687793,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=3500 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.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 --subproc-heap-profiling --metrics-shmem-handle=3480,i,13567821419810736744,11835255301296627806,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=5676 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.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 --subproc-heap-profiling --metrics-shmem-handle=3456,i,880953565732450865,11054653322098943300,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=3488 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --force-high-res-timeticks=disabled --subproc-heap-profiling --metrics-shmem-handle=5852,i,11488044612722313915,10847716435878803633,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=5860 /prefetch:12
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --subproc-heap-profiling --metrics-shmem-handle=5884,i,17369766105558565846,8842617094398236132,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=5888 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --subproc-heap-profiling --disable-gpu-compositing --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=22 --metrics-shmem-handle=3500,i,17745922555854456540,15002458487766714833,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=4364 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --subproc-heap-profiling --metrics-shmem-handle=4276,i,5191311218221556826,5441037294664232593,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=5688 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --subproc-heap-profiling --disable-gpu-compositing --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=24 --metrics-shmem-handle=6112,i,6177522636145493945,2114482096302928855,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=6116 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --subproc-heap-profiling --metrics-shmem-handle=6288,i,10462643705939757314,12993539892433392559,524288 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=6304 /prefetch:14
```

C:\Program Files\Internet Explorer\iexplore.exe

```
"C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\Admin\Desktop\ResolveTest.gif
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" -- "file:///C:/Users/Admin/Desktop/ResolveTest.gif"
```

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=10 --always-read-main-dll --metrics-shmem-handle=4828,i,1153041881255284177,4997686573283337664,2097152 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=5032 /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=9 --always-read-main-dll --metrics-shmem-handle=4500,i,10029922810695995598,11925349319620339425,2097152 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=5092 /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=5196,i,12244502105518278491,8793938013533415001,524288 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=5480 /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=4852,i,12688174458652689383,10594931656981384772,524288 --field-trial-handle=2708,i,9368923709298212835,3269444283866718709,262144 --variations-seed-version --mojo-platform-channel-handle=5504 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window
```

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=0x23c,0x240,0x244,0x238,0x250,0x7ffbeb97c188,0x7ffbeb97c194,0x7ffbeb97c1a0
```

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=1724,i,1630448158874452559 8,1807306457141063757 2,524288 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=2148 /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=SAAAAAAAAADgAAAIAAAAAAAAAAAAGAAAQAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --always-read-main-dll --metrics-shmem-handle=1496,i,11465332734896303891,6576597274736387095,262144 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=2116 /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=2380,i,8480152640997301290,17039558156490997611,524288 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=2288 /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\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=4500,i,6983445746685522601,2934246772049542344,524288 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=4516 /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=4500,i,6983445746685522601,2934246772049542344,524288 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=4516 /prefetch:14
```

C:\Program Files\VideoLAN\VLC\vlc.exe

```
"C:\Program Files\VideoLAN\VLC\vlc.exe" --started-from-file "C:\Users\Admin\Desktop\LockTest.mp4"
```

C:\Windows\system32\OpenWith.exe

```
C:\Windows\system32\OpenWith.exe -Embedding
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument C:\Users\Admin\Desktop\OutRemove.pdf
```

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=4976,i,12945377829438903472,11700838078919000597,2097152 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=5052 /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=6 --always-read-main-dll --metrics-shmem-handle=5016,i,17235696013361775561,17701295062369841135,2097152 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=5060 /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=5544,i,1928153235151510433,14050360154486841077,524288 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=5560 /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=5548,i,8637855149861452898,1013232250525307749,524288 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=5612 /prefetch:14
```

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 --init-isolate-as-foreground --pdf-shared-library --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=10 --always-read-main-dll --metrics-shmem-handle=5916,i,3040129164847877190,4367442847071121146,2097152 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=5920 /prefetch:9
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --renderer-sub-type=pdf-renderer --pdf-renderer --pdf-shared-library --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= --jitless" --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=11 --always-read-main-dll --metrics-shmem-handle=6160,i,1768948702799350049,5451200807593660928,2097152 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=6112 /prefetch:15
```

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 --init-isolate-as-foreground --pdf-shared-library --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=12 --always-read-main-dll --metrics-shmem-handle=4996,i,14964466201920067693,16221559362248578035,2097152 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=6540 /prefetch:9
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --renderer-sub-type=pdf-renderer --pdf-renderer --pdf-shared-library --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= --jitless" --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=13 --always-read-main-dll --metrics-shmem-handle=6228,i,13307748862389001993,17787189463757717149,2097152 --field-trial-handle=2120,i,11677828753883233696,9486175495513079833,262144 --variations-seed-version --mojo-platform-channel-handle=6268 /prefetch:15
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window
```

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=0x23c,0x240,0x244,0x238,0x2f0,0x7ffbeb97c188,0x7ffbeb97c194,0x7ffbeb97c1a0
```

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=1812,i,11814792964500222666,13457382530945106998,524288 --field-trial-handle=2496,i,4428679896889529889,18086839243183666592,262144 --variations-seed-version --mojo-platform-channel-handle=2640 /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=SAAAAAAAAADgAAAIAAAAAAAAAAAAAGAAAQAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --always-read-main-dll --metrics-shmem-handle=1516,i,17116710986457242387,8054026327430903 79,262144 --field-trial-handle=2496,i,4428679896889529889,18086839243183666592,262144 --variations-seed-version --mojo-platform-channel-handle=2480 /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 --no-pre-read-main-dll --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=2184,i,3565266311606020049,8858539238563033163,524288 --field-trial-handle=2496,i,4428679896889529889,18086839243183666592,262144 --
variations-seed-version --mojo-platform-channel-handle=2488 /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\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=4464,i,13937405182354549245,12992496509087299141,524288 --field-trial-
handle=2496,i,4428679896889529889,18086839243183666592,262144 --variations-seed-version --mojo-platform-channel-handle=4480 /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=4464,i,13937405182354549245,12992496509087299141,524288 --field-trial-
handle=2496,i,4428679896889529889,18086839243183666592,262144 --variations-seed-version --mojo-platform-channel-handle=4480 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-
timeticks=disabled --subproc-heap-profiling --disable-gpu-compositing --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=26 --metrics-shmem-
handle=4720,i,4540188246183591672,3327861614151575286,2097152 --field-trial-handle=2092,i,3625966286463297903,9294234558738065328,262144 --
variations-seed-version=20260129-170056.646000 --mojo-platform-channel-handle=4792 /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=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=4540,i,17906408041895663264,15234930725378386543,524288 --field-trial-handle=2496,i,4428679896889529889,18086839243183666592,262144
--variations-seed-version --mojo-platform-channel-handle=4800 /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=4768,i,6384191790801453410,11881393435821770350,524288 --field-trial-handle=2496,i,4428679896889529889,18086839243183666592,262144 -
-variations-seed-version --mojo-platform-channel-handle=4780 /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=4548,i,2174181061764574257,17938672028217408065,524288 --field-trial-handle=2496,i,4428679896889529889,18086839243183666592,262144 -
-variations-seed-version --mojo-platform-channel-handle=4856 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe"
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-
dir=C:\Users\Admin\AppData\Local\Google\Chrome\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--
database=C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Crashpad" "--metrics-dir=C:\Users\Admin\AppData\Local\Google\Chrome\User
Data" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --
annotation=ver=140.0.7339.81 --initial-client-data=0xfc,0x100,0x104,0xd8,0x108,0x7ffbf20cc728,0x7ffbf20cc734,0x7ffbf20cc740
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=gpu-process --no-pre-read-main-dll --force-high-res-timeticks=disabled --
gpu-preferences=SAAAAAAAAADgAAAIAAAAAAAAAAAAAGAAAQAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --
metrics-shmem-handle=1568,i,661710150185564254,14138505604494777087,262144 --field-trial-
handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-
channel-handle=1908 /prefetch:2
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --
service-sandbox-type=none --force-high-res-timeticks=disabled --metrics-shmem-
handle=2204,i,17577407972308417063,12531394358986885609,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 -
-variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=2220 /prefetch:11
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --
service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-
handle=2368,i,13405552782685255096,15616620737055305963,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 -
-variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=1784 /prefetch:13
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --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=6 --metrics-shmem-handle=3196,i,5275053031370245209,14882797719312923420,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=3404 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --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 --metrics-shmem-handle=3328,i,8433217210929880278,10685133137880401960,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=3440 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\140.0.7339.81\elevation_service.exe

```
"C:\Program Files\Google\Chrome\Application\140.0.7339.81\elevation_service.exe"
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-handle=4492,i,10183120613186629019,15557442528199813494,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=4380 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=8 --metrics-shmem-handle=4564,i,1910015090817621534,8835136969029773258,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=4580 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-handle=4716,i,13488097807534019464,16199685944398902953,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=4724 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.ProcessorMetrics --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --metrics-shmem-handle=5188,i,5542599547548853063,8435412184692016998,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5184 /prefetch:14
```

C:\Windows\system32\svchost.exe

```
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s NgcSvc
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=11 --metrics-shmem-handle=5228,i,11229448505373380090,1417996005827359019,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5452 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=12 --metrics-shmem-handle=3568,i,1442829585274811341,4273670217827090017,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=3656 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --force-high-res-timeticks=disabled --metrics-shmem-handle=3400,i,16220112033627968655,1476702633605512136,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=3044 /prefetch:12
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --metrics-shmem-handle=3672,i,9033297916966014218,14398928455866334738,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5588 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.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 --metrics-shmem-handle=5756,i,2972362619805556895,17724945056090750295,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5808 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.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 --metrics-shmem-handle=5780,i,14641283998014410804,17338729693160338957,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5800 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.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 --metrics-shmem-handle=5796,i,5342205083024320520,5927654776426893745,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5736 /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=SAAAAAAAAADoAAAIAAAAAAAAAAAAAGAAAQAAAAAAAACEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --always-read-main-dll --metrics-shmem-handle=4652,i,15936383765389954345,1283311804033886256,262144 --field-trial-handle=2496,i,4428679896889529889,18086839243183666592,262144 --variations-seed-version --mojo-platform-channel-handle=5008 /prefetch:10
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=19 --metrics-shmem-handle=5872,i,86184220597796228 67,9033085110378043348,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5800 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-handle=5924,i,12108129990614995603,10872677782859304679,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5728 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=21 --metrics-shmem-handle=6056,i,5932984658346791857,1256405127038764510,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6080 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-handle=6188,i,12128149071462586006,6820533789750781738,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6164 /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=4292,i,10999918311951801552,12144576976292556858,524288 --field-trial-handle=2496,i,4428679896889529889,18086839243183666592,262144 --variations-seed-version --mojo-platform-channel-handle=3592 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.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=SAAAAAAAAADoAAAIAAAAAAAAAAAAAGAAAQAAAAAAAACEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --metrics-shmem-handle=5420,i,6671588855243285445,17777278260025042150,262144 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6272 /prefetch:10
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=24 --metrics-shmem-handle=6212,i,8281825647824788632,4168548509328650277,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=876 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-
timeticks=disabled --disable-gpu-compositing --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=25 --metrics-shmem-
handle=3512,i,6724074431170467194,18340049690414399066,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 -
-variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6328 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-
US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-
handle=5844,i,7778633419020254420,4840894162576742134,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --
variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=3596 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-
timeticks=disabled --disable-gpu-compositing --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=27 --metrics-shmem-
handle=6332,i,10913475225083958834,11831880941513888973,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144
--variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=3588 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-
US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-
handle=6020,i,11563280840729660596,10646348334561490949,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 -
-variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5772 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-
timeticks=disabled --disable-gpu-compositing --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=29 --metrics-shmem-
handle=6356,i,13378032743258945066,7562855156415574576,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 -
-variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6456 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.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 --metrics-shmem-
handle=3640,i,10235890774573708726,9727214005494734808,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --
variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=3480 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-
timeticks=disabled --disable-gpu-compositing --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=31 --metrics-shmem-
handle=3628,i,170233595306312183,15039921321552337701,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --
variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5748 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-
US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-
handle=5780,i,17644681171910892116,12023674683234582655,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 -
-variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5828 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-
timeticks=disabled --disable-gpu-compositing --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=33 --metrics-shmem-
handle=3596,i,2148754652164477283,11171702946571405933,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 -
-variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5852 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-
US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-
handle=6676,i,10625319476717750599,2126605096543420275,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --
variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6648 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-
timeticks=disabled --disable-gpu-compositing --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=35 --metrics-shmem-
handle=6684,i,8165793659492451954,15633920420223996762,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 -
-variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=3644 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=36 --metrics-shmem-handle=6440,i,8477894057315426493,4263882092963691992,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6204 /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=3744,i,2327154939201743545,16906147523231562323,524288 --field-trial-handle=2496,i,4428679896889529889,18086839243183666592,262144 --variations-seed-version --mojo-platform-channel-handle=4100 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=37 --metrics-shmem-handle=6376,i,4292603406711337339,10020805278914097755,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=3568 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-handle=6436,i,2252959560487561774,13803785273241462464,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6328 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=39 --metrics-shmem-handle=6492,i,5159963492258789717,10840985456265273789,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6276 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --metrics-shmem-handle=7008,i,9526599059873359035,7990590201604282005,524288 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=7016 /prefetch:14
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=41 --metrics-shmem-handle=7096,i,18413263249924846556,6739569132715021520,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=7188 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=42 --metrics-shmem-handle=6900,i,5610986454563723452,15599004527033193125,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=6904 /prefetch:1
```

C:\Program Files\Google\Chrome\Application\chrome.exe

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=renderer --enable-dinosaur-easter-egg-alt-images --force-high-res-timeticks=disabled --disable-gpu-compositing --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=43 --metrics-shmem-handle=7056,i,16459274823091646023,967282051611837027,2097152 --field-trial-handle=1912,i,1826249946666543244,5811382326459004100,262144 --variations-seed-version=20260214-030037.053000-production --mojo-platform-channel-handle=5728 /prefetch:1
```

4. 5. Network

Country	Destination	Domain	Proto
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	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	copilot.microsoft.com	udp
US	8.8.8.8:53	copilot.microsoft.com	udp
US	150.171.27.11:80	edge.microsoft.com	tcp
US	150.171.109.210:443	apps.microsoft.com	tcp

US	150.171.109.210:443	apps.microsoft.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	104.18.23.222:443	copilot.microsoft.com	udp
US	104.18.23.222:443	copilot.microsoft.com	tcp
US	150.171.109.210:443	apps.microsoft.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	150.171.109.210:443	apps.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
GB	23.37.196.9:443	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
US	8.8.8.8:53	wcpstatic.microsoft.com	udp
US	8.8.8.8:53	wcpstatic.microsoft.com	udp
US	8.8.8.8:53	sparkcdneus2.azureedge.net	udp
US	8.8.8.8:53	sparkcdneus2.azureedge.net	udp
GB	23.37.196.9:443	musicart.xboxlive.com	tcp
US	150.171.109.214:443	wcpstatic.microsoft.com	tcp
US	150.171.109.214:443	wcpstatic.microsoft.com	tcp
US	150.171.109.210:443	apps.microsoft.com	tcp
US	8.8.8.8:53	js.monitor.azure.com	udp
US	8.8.8.8:53	js.monitor.azure.com	udp
US	8.8.8.8:53	www.clarity.ms	udp
US	8.8.8.8:53	www.clarity.ms	udp
US	150.171.109.215:443	js.monitor.azure.com	tcp
US	150.171.109.215:443	js.monitor.azure.com	tcp
CH	20.250.198.32:443	www.clarity.ms	tcp
US	8.8.8.8:53	scripts.clarity.ms	udp
US	8.8.8.8:53	scripts.clarity.ms	udp
US	150.171.109.210:443	scripts.clarity.ms	tcp
US	8.8.8.8:53	login.microsoftonline.com	udp
US	8.8.8.8:53	login.microsoftonline.com	udp
US	8.8.8.8:53	login.microsoftonline.com	udp
US	8.8.8.8:53	login.microsoftonline.com	udp
IE	20.190.159.68:443	login.microsoftonline.com	tcp
NL	20.190.160.14:443	login.microsoftonline.com	tcp
US	8.8.8.8:53	i.clarity.ms	udp
US	8.8.8.8:53	i.clarity.ms	udp
US	150.171.109.210:443	scripts.clarity.ms	tcp
US	4.153.72.49:443	i.clarity.ms	tcp
US	150.171.28.11:443	edge.microsoft.com	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	52.168.112.66:443	browser.events.data.microsoft.com	tcp
US	150.171.109.210:443	scripts.clarity.ms	tcp
US	52.168.112.66:443	browser.events.data.microsoft.com	tcp
GB	2.16.153.206:443	www.bing.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	52.240.245.68:443	northcentralus-0.in.applicationinsights.azure.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.27.11:443	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	150.171.109.216:443	edgeassetservice.azureedge.net	tcp
US	150.171.109.216:443	edgeassetservice.azureedge.net	tcp
US	150.171.109.210:443	scripts.clarity.ms	tcp
N/A	224.0.0.251:5353		udp
US	4.153.72.49:443	i.clarity.ms	tcp
US	4.153.72.49:443	i.clarity.ms	tcp
US	150.171.109.210:443	scripts.clarity.ms	tcp

US	52.240.245.68:443	northcentralus-0.in.applicationinsights.azure.com	tcp
US	8.8.8.8:53	get.microsoft.com	udp
US	8.8.8.8:53	get.microsoft.com	udp
GB	2.16.55.65:443	get.microsoft.com	tcp
US	52.168.112.66:443	browser.events.data.microsoft.com	tcp
US	52.168.112.66:443	browser.events.data.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	150.171.109.213:443	edge-consumer-static.azureedge.net	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	update.googleapis.com	udp
US	8.8.8.8:53	update.googleapis.com	udp
US	8.8.8.8:53	sparkcdneus2.azureedge.net	udp
US	8.8.8.8:53	sparkcdneus2.azureedge.net	udp
GB	23.37.196.9:443	musicart.xboxlive.com	tcp
GB	23.37.196.9:443	musicart.xboxlive.com	tcp
CH	20.250.198.32:443	www.clarity.ms	tcp
IE	20.190.159.68:443	login.microsoftonline.com	tcp
NL	20.190.160.14:443	login.microsoftonline.com	tcp
US	150.171.109.215:443	js.monitor.azure.com	tcp
US	8.8.8.8:53	sparkcdneus2.azureedge.net	udp
US	8.8.8.8:53	sparkcdneus2.azureedge.net	udp
GB	23.37.196.9:443	musicart.xboxlive.com	tcp
GB	23.37.196.9:443	musicart.xboxlive.com	tcp
US	8.8.8.8:53	static.edge.microsoftapp.net	udp
US	8.8.8.8:53	static.edge.microsoftapp.net	udp
US	150.171.109.214:443	static.edge.microsoftapp.net	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
GB	2.16.55.53:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
GB	2.16.153.206:443	www.bing.com	udp
US	8.8.8.8:53	i.clarity.ms	udp
US	8.8.8.8:53	i.clarity.ms	udp
GB	142.250.151.94:80	c.pki.goog	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	northcentralus-0.in.applicationinsights.azure.com	udp
US	8.8.8.8:53	northcentralus-0.in.applicationinsights.azure.com	udp
GB	2.16.153.206:443	www.bing.com	udp
US	8.8.8.8:53	i.clarity.ms	udp
US	8.8.8.8:53	i.clarity.ms	udp
US	4.153.72.49:443	i.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	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	i.clarity.ms	udp
US	8.8.8.8:53	i.clarity.ms	udp
US	4.153.72.49:443	i.clarity.ms	tcp
US	8.8.8.8:53	i.clarity.ms	udp
US	8.8.8.8:53	i.clarity.ms	udp
US	4.153.72.49:443	i.clarity.ms	tcp
GB	2.16.153.224:443	www.bing.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
GB	2.16.153.224:443	www.bing.com	tcp
US	8.8.8.8:53	ntp.msn.com	udp
US	8.8.8.8:53	ntp.msn.com	udp
GB	96.17.179.184:443	ntp.msn.com	tcp
GB	96.17.179.184:443	ntp.msn.com	tcp
US	8.8.8.8:53	xpaywalletcdn-prod.azureedge.net	udp
US	8.8.8.8:53	xpaywalletcdn-prod.azureedge.net	udp
US	8.8.8.8:53	assets.msn.com	udp
US	8.8.8.8:53	assets.msn.com	udp
US	150.171.109.216:443	xpaywalletcdn-prod.azureedge.net	tcp

GB	104.79.93.250:443	assets.msn.com	tcp
GB	104.79.93.250:443	assets.msn.com	tcp
US	8.8.8.8:53	img-s-msn-com.akamaized.net	udp
US	8.8.8.8:53	sb.scorecardresearch.com	udp
US	8.8.8.8:53	sb.scorecardresearch.com	udp
US	8.8.8.8:53	th.bing.com	udp
US	8.8.8.8:53	th.bing.com	udp
US	8.8.8.8:53	c.msn.com	udp
US	8.8.8.8:53	c.msn.com	udp
US	8.8.8.8:53	c.bing.com	udp
US	8.8.8.8:53	c.bing.com	udp
US	150.171.27.10:443	c.bing.com	tcp
GB	2.16.153.206:443	www.bing.com	tcp
US	150.171.109.216:443	c.msn.com	tcp
GB	2.16.153.206:443	www.bing.com	tcp
FR	52.222.169.76:443	sb.scorecardresearch.com	tcp
GB	2.16.55.202:443	img-s-msn-com.akamaized.net	tcp
US	8.8.8.8:53	browser.events.data.msn.com	udp
US	8.8.8.8:53	browser.events.data.msn.com	udp
US	20.189.173.26:443	browser.events.data.msn.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	20.189.173.26:443	browser.events.data.msn.com	tcp
US	20.189.173.26:443	browser.events.data.msn.com	tcp
US	20.189.173.26:443	browser.events.data.msn.com	tcp
US	8.8.8.8:53	srtb.msn.com	udp
US	8.8.8.8:53	srtb.msn.com	udp
US	204.79.197.203:443	srtb.msn.com	tcp
GB	2.16.55.202:443	img-s-msn-com.akamaized.net	udp
US	8.8.8.8:53	r.bing.com	udp
US	8.8.8.8:53	th.bing.com	udp
US	8.8.8.8:53	th.bing.com	udp
GB	2.16.153.206:443	th.bing.com	tcp
GB	2.16.153.206:443	th.bing.com	tcp
GB	2.16.153.224:443	th.bing.com	tcp
GB	2.16.153.224:443	th.bing.com	tcp
GB	2.16.153.206:443	th.bing.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
GB	2.16.153.206:443	th.bing.com	udp
GB	2.16.153.206:443	th.bing.com	udp
GB	2.16.153.224:443	th.bing.com	udp
US	8.8.8.8:53	challenges.cloudflare.com	udp
US	8.8.8.8:53	challenges.cloudflare.com	udp
US	104.18.94.41:443	challenges.cloudflare.com	udp
GB	2.16.153.206:443	th.bing.com	udp
US	8.8.8.8:53	login.microsoftonline.com	udp
US	8.8.8.8:53	login.microsoftonline.com	udp
IE	40.126.31.71:443	login.microsoftonline.com	tcp
US	8.8.8.8:53	challenges.cloudflare.com	udp
US	8.8.8.8:53	challenges.cloudflare.com	udp
US	104.18.95.41:443	challenges.cloudflare.com	tcp
US	104.18.95.41:443	challenges.cloudflare.com	tcp
US	104.18.95.41:443	challenges.cloudflare.com	udp
GB	52.109.28.47:443	roaming.svc.cloud.microsoft	tcp
US	204.79.197.203:443	srtb.msn.com	tcp
US	8.8.8.8:53	r.bing.com	udp
US	8.8.8.8:53	r.bing.com	udp
US	8.8.8.8:53	r.msftstatic.com	udp
US	8.8.8.8:53	r.msftstatic.com	udp
US	204.79.197.219:443	r.msftstatic.com	tcp
US	204.79.197.219:443	r.msftstatic.com	tcp
GB	2.16.153.206:443	r.bing.com	tcp
GB	2.16.153.206:443	r.bing.com	tcp
US	20.189.173.26:443	browser.events.data.msn.com	tcp

GB	2.16.153.206:443	r.bing.com	udp
GB	2.16.153.224:443	r.bing.com	udp
US	8.8.8.8:53	i.clarity.ms	udp
US	8.8.8.8:53	i.clarity.ms	udp
US	4.153.72.49:443	i.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	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
GB	2.16.153.224:443	www.bing.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
GB	2.16.153.224:443	www.bing.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
GB	2.16.153.224:443	www.bing.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
GB	2.16.153.224:443	www.bing.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	www.google.com	udp
NL	192.178.223.104:443	www.google.com	tcp
NL	192.178.223.104:443	www.google.com	tcp
NL	192.178.223.104:443	www.google.com	tcp
NL	192.178.223.104:443	www.google.com	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	udp
GB	142.250.117.95:443	content-autofill.googleapis.com	tcp
GB	142.250.151.101:443	encrypted-tbn1.gstatic.com	udp
GB	142.250.151.101:443	encrypted-tbn1.gstatic.com	tcp
GB	142.250.151.101:443	encrypted-tbn1.gstatic.com	udp
NL	192.178.223.104:443	www.google.com	udp
NL	192.178.223.104:443	www.google.com	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	tcp
NL	192.178.223.104:443	www.google.com	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	udp
US	8.8.8.8:53	edge-consumer-static.azureedge.net	udp
US	8.8.8.8:53	edge-consumer-static.azureedge.net	udp
GB	142.250.151.101:443	encrypted-tbn1.gstatic.com	tcp
US	13.107.226.64:443	edge-consumer-static.azureedge.net	tcp
GB	142.250.151.101:443	encrypted-tbn1.gstatic.com	udp
NL	192.178.223.139:443	consent.google.com	tcp
NL	192.178.223.84:443	accounts.google.com	udp
GB	142.250.117.95:443	content-autofill.googleapis.com	udp
GB	142.250.129.113:443	ogs.google.com	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	udp
GB	142.250.151.101:443	encrypted-tbn1.gstatic.com	udp
US	8.8.8.8:53	api.edgeoffer.microsoft.com	udp
US	8.8.8.8:53	api.edgeoffer.microsoft.com	udp
US	150.171.109.212:443	api.edgeoffer.microsoft.com	tcp
US	150.171.109.212:443	api.edgeoffer.microsoft.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.27.11:443	edge.microsoft.com	tcp
GB	2.16.153.224:443	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	150.171.27.11:443	edge.microsoft.com	tcp
GB	2.16.153.224:443	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	150.171.27.11:443	edge.microsoft.com	tcp
GB	2.16.153.224:443	www.bing.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp

US	150.171.27.11:443	edge.microsoft.com	tcp
GB	2.16.153.224:443	www.bing.com	tcp
US	8.8.8.8:53	api.edgeoffer.microsoft.com	udp
US	8.8.8.8:53	api.edgeoffer.microsoft.com	udp
US	150.171.109.214:443	api.edgeoffer.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
GB	2.16.153.206:443	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	150.171.28.11:443	edge.microsoft.com	tcp
GB	2.16.153.206:443	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	150.171.28.11:443	edge.microsoft.com	tcp
GB	2.16.153.206:443	www.bing.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
GB	2.16.153.206:443	www.bing.com	tcp
NL	192.178.223.84:443	accounts.google.com	udp
GB	142.250.117.94:443	google.co.uk	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	udp
GB	142.250.117.95:443	content-autofill.googleapis.com	udp
GB	142.250.117.95:443	content-autofill.googleapis.com	tcp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	udp
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	150.171.109.210:443	edge-consumer-static.azureedge.net	tcp
US	8.8.8.8:53	static.edge.microsoftapp.net	udp
US	8.8.8.8:53	static.edge.microsoftapp.net	udp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	150.171.109.214:443	static.edge.microsoftapp.net	tcp
US	142.251.157.119:443	www.google.com	tcp
US	142.251.157.119:443	www.google.com	tcp
US	142.251.157.119:443	www.google.com	tcp
US	142.251.157.119:443	www.google.com	tcp
US	142.251.157.119:443	www.google.com	tcp
US	142.251.157.119:443	www.google.com	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	udp
GB	142.250.117.95:443	content-autofill.googleapis.com	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	tcp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	udp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	tcp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	udp
GB	142.250.117.95:443	content-autofill.googleapis.com	tcp
GB	142.250.140.102:443	encrypted-tbn0.gstatic.com	tcp
GB	142.250.140.102:443	encrypted-tbn0.gstatic.com	tcp
GB	142.250.140.102:443	encrypted-tbn0.gstatic.com	tcp
GB	142.250.117.95:443	content-autofill.googleapis.com	udp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.129.190:443	www.youtube.com	tcp
GB	142.250.129.190:443	www.youtube.com	udp
GB	142.250.129.190:443	www.youtube.com	tcp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	udp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	tcp
GB	142.250.129.190:443	www.youtube.com	udp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	udp
GB	142.250.151.119:443	i.ytimg.com	tcp
GB	142.250.151.154:443	googleads.g.doubleclick.net	tcp
GB	142.250.140.148:443	static.doubleclick.net	tcp
GB	142.250.151.154:443	googleads.g.doubleclick.net	udp
US	142.251.157.119:443	www.google.com	tcp
GB	142.250.140.95:443	content-autofill.googleapis.com	tcp

GB	142.250.140.95:443	content-autofill.googleapis.com	udp
CA	34.130.135.16:443	e2c21.gcp.gvt2.com	tcp
HU	172.217.20.35:443	beacons.gvt2.com	tcp
GB	142.250.117.154:443	googleads.g.doubleclick.net	udp
GB	142.250.117.154:443	googleads.g.doubleclick.net	udp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.140.102:443	encrypted-tbn0.gstatic.com	udp
GB	142.250.140.95:443	content-autofill.googleapis.com	udp
GB	142.250.140.95:443	content-autofill.googleapis.com	udp
GB	142.250.140.95:443	content-autofill.googleapis.com	tcp
GB	142.250.151.119:443	i.ytimg.com	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	udp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	udp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	tcp
GB	142.250.140.95:443	content-autofill.googleapis.com	udp
NL	192.178.223.99:443	www.google.com	udp
GB	142.250.129.132:443	lh3.googleusercontent.com	tcp
GB	142.250.129.132:443	lh3.googleusercontent.com	tcp
GB	142.250.129.132:443	lh3.googleusercontent.com	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
NL	192.178.223.99:443	www.google.com	udp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.151.139:443	encrypted-tbn1.gstatic.com	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.117.101:443	google.com	tcp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.129.102:443	ogs.google.com	tcp
FR	3.165.113.70:443	www.biblegateway.com	tcp
FR	3.165.113.70:443	www.biblegateway.com	tcp
US	104.18.86.42:443	cdn.cookielaw.org	tcp
US	104.18.86.42:443	cdn.cookielaw.org	tcp
GB	142.251.30.95:443	content-autofill.googleapis.com	tcp
US	172.64.155.119:443	geolocation.onetrust.com	tcp
GB	142.251.30.95:443	content-autofill.googleapis.com	udp
MX	34.51.10.38:443	e2c80.gcp.gvt2.com	tcp
HU	172.217.20.35:443	beacons.gvt2.com	udp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
GB	142.250.140.138:443	encrypted-tbn0.gstatic.com	udp
GB	142.250.140.95:443	content-autofill.googleapis.com	udp
GB	142.250.140.95:443	content-autofill.googleapis.com	udp
GB	142.250.140.95:443	content-autofill.googleapis.com	tcp
GB	142.250.129.119:443	i.ytimg.com	tcp
GB	142.250.129.93:443	www.youtube.com	udp
GB	142.251.29.95:443	content-autofill.googleapis.com	udp
US	216.239.34.157:443	tunnel.googlezip.net	tcp
FR	18.245.201.4:443	images-eu.ssl-images-amazon.com	tcp
FR	18.245.201.4:443	images-eu.ssl-images-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	udp
FR	143.204.196.147:443	m.media-amazon.com	udp
FR	18.245.201.4:443	images-eu.ssl-images-amazon.com	udp

IE	52.16.118.74:443	fls-eu.amazon.co.uk	tcp
FR	18.245.201.4:443	images-eu.ssl-images-amazon.com	tcp
FR	18.155.125.32:443	www.amazon.co.uk	tcp
GB	142.250.129.95:443	content-autofill.googleapis.com	tcp
FR	18.245.201.4:443	images-eu.ssl-images-amazon.com	udp
FR	52.222.201.128:443	dcp-rf1.amazon.co.uk	tcp
FR	13.227.173.22:443	read.amazon.co.uk	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	143.204.196.147:443	m.media-amazon.com	tcp
FR	3.162.38.28:443	rf-completion.amazon.co.uk	tcp
FR	18.155.125.32:443	www.amazon.co.uk	udp
FR	52.222.201.128:443	dcp-rf1.amazon.co.uk	tcp
ES	15.216.144.236:443	api.stores.eu-south-2.prod.paets.advertising.amazon.dev	tcp
FR	143.204.196.147:443	m.media-amazon.com	udp
FR	52.222.149.66:443	aax-eu-zaz.amazon.co.uk	tcp
IE	3.254.238.163:443	unagi.amazon.co.uk	tcp
FR	3.165.135.164:443	d3umadsut2tsh9.cloudfront.net	tcp
FR	3.165.135.164:443	d3umadsut2tsh9.cloudfront.net	tcp
FR	3.165.135.164:443	d3umadsut2tsh9.cloudfront.net	tcp

4. 6. Files

memory/4908-0-0x000001EE75CE0000-0x000001EE75DEE000-memory.dmp

memory/4908-1-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-2-0x000001EE76330000-0x000001EE7633A000-memory.dmp

memory/4908-3-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-4-0x000001EE78E50000-0x000001EE78F0A000-memory.dmp

C:\Users\Admin\AppData\Local\Temp\Tmp14AC.tmp

MD5	a10f31fa140f2608ff150125f3687920
SHA1	ec411cc7005aaa8e3775cf105fcd4e1239f8ed4b
SHA256	28c871238311d40287c51dc09aee6510cac5306329981777071600b1112286c6
SHA512	cf915fb34cd5ecfbd6b25171d6e0d3d09af2597edf29f9f24fa474685d4c5ec9bc742ade9f29abac457dd645ee955b1914a635c90af77c519d2ada895e7ecf12

memory/4908-15-0x000001EE77CA0000-0x000001EE77CB2000-memory.dmp

memory/4908-16-0x000001EE78600000-0x000001EE7863C000-memory.dmp

memory/4908-17-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-18-0x000001EE78DF0000-0x000001EE78E16000-memory.dmp

memory/4908-19-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-20-0x000001EE7B3F0000-0x000001EE7B428000-memory.dmp

memory/4908-22-0x000001EE791D0000-0x000001EE791D8000-memory.dmp

memory/4908-21-0x000001EE7B430000-0x000001EE7B43E000-memory.dmp

memory/4908-23-0x000001EE7BDD0000-0x000001EE7BF58000-memory.dmp

memory/4908-24-0x000001EE7BD50000-0x000001EE7BD58000-memory.dmp

memory/4908-25-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-26-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-27-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-28-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-29-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-30-0x000001EE761F0000-0x000001EE761FC000-memory.dmp

memory/4908-31-0x000001EE77C60000-0x000001EE77C72000-memory.dmp

memory/4908-32-0x000001EE78680000-0x000001EE78690000-memory.dmp

memory/4908-36-0x000001EE761F0000-0x000001EE761FC000-memory.dmp

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

MD5	fb7d9391eb1040937b5c31ff61febe79
SHA1	0be0bde544b492ac590e441f96bf8d0a378d3782
SHA256	5d8c0ebc33f7882ac8aaa0f941413384749c7672a7744de3485d53f3d7a832ce
SHA512	d4a405f080afee18100d407e824cc3366114b1acd56307d247bc25ee87ffaba37406581a2dfcfe9320df4d014582f86fd300e9f67a54b4fcd2e471e1358c493d

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

MD5	eaf65f57619b5bfb175d7cef9ee4940e
SHA1	9eb9e57601fc137a652213d2302a2f0dc0dbfad9
SHA256	9a0e51d72fdefce5748786dc938275d3eeea5f628b3f4eae29befdceee483ef9
SHA512	993fc6b5767343aa1c78558920a4e84a7b07987d25a39303d77235f430835e1038484c50128f5cb0dd6dfe94530344efb8d884df56024930e525b49f97b3fc9d

\??\pipe\crashpad_5772_GBCUHBFXOQIROHZP

MD5	d41d8cd98f00b204e9800998ecf8427e
SHA1	da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA256	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA512	cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e

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

MD5	2ee9c9062df63fee32f65bc087b93005
SHA1	2874f6b34fdb5f9ff64aed6e38005f7940050b27
SHA256	71f86f37b013034051fae2e3307728bc40653c617383d6aa85219dd8ea093ca3
SHA512	99729f971f840d780b0e5404260284b048d532cb0dbd20969536cacd61a2d2c52568d6b9d96f6f0168b93eaa3c7236b49d8aafb6138d1b1fcbe89990c6af5af3

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	08f4b7af1615089ada945074d0b8ca89
SHA1	e489bb17658c3fa0d12b133477d0f7999b57d501
SHA256	fe634aa68607bb8a1f3c9e0ea69deb3f0e6f61fb7e7e660a1810134768a49097
SHA512	8a63c9d5ed014d1c617341499222f04dca2f197c03acd0e71aefc5aff86bdcd33642e0e9d1ad1ba064da2d7367177421c0b2f33008668a03d7acdc7d84780f2d

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\index.txt~RFe585484.TMP

MD5	63012766794c16ecd13d07e879896c83
SHA1	006c79ded3c3f4d2fe2a5f3d00ed28fc3ec33f5e
SHA256	d39f9ac36ffc89d7d4b5207e02367cb0a1552c3d53f845a202d1c912c6024f04
SHA512	220421f51388adc054a688d6bc414bb626c36f9a315a471e0b520642509db00b822c3e21f909e03b9f52457649f0e41a391f5983aeef0f1abe2efddd97e02317

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

MD5	3ead9bc59467e00cb8497f9c3cd89fb6
SHA1	9cff51febb92b61168c4758dc4518f9711435331
SHA256	fbca36ed77436b1aaaac56529314efd11baa4d49946bc7ed0ce497d3d89b455c
SHA512	a8cbf06f54f344497555f61d83d80738227696a242479532138ea830bf9704ced9b93cdb80f95e21504e244079f4112bd837e54de66133ff6cea54e4a7f40d79

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\Microsoft\Edge\User Data\Default\HubApps

MD5	35ae3b10ff09df4a55dc35b6a13e7f7a
SHA1	fe687665d50274195c09df8c0da43a3281143963
SHA256	a3e0ed3b7b22eb63f8d684039026c6d1cf309dea226c1060864a6dde8ef4297c
SHA512	6e0f0955ecc244ee48e49a902266addd795478331bd0f0865b92d66a08f660efe55cd0ca570f6116b5ba85970c359854e921faf3b517b566cbdc2ec1c6e7719b

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\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\Local State

MD5	1b77c7a3543211ed50065916a3482d9c
SHA1	af80a311dbd64287b7eecdb901e6fad769b77200
SHA256	68dd6b6e4e5d403d47a6d1bd7c4f2a338c1e6314a9ceeae07255906e1ef628dd
SHA512	ca4e6683e037d1fa98b0832aaa2f27d6bf6987c5c1de9be56fd181a58b3da1359215a211724756028ab4bd5f9ee7d77578847c08a783974e0e09adc119a9cdda

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

MD5	5c49fb64278ae7e588a3d40fe751cd8f
SHA1	31df8f697bf52d280bfe88d8a072e794fef9eef5
SHA256	3db0d5fda7da57451e21b629ad7265936a866fe927d70f16e88ad491274c5bcc
SHA512	cabc49f8e5b8af953b08e5fe6d97c8ddec5d44d5ac3c0c192caea6715eba8acfd556d906b62ac281fb9d33614f0cc50b0620c845fede8d2e55dff30d386cc3b1

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

MD5	cf55932a0f0c4c92add688b71e99899b
SHA1	1a93b1976d665a097b2a14b758bb6cc04f9db982
SHA256	e8816bfd77080603cca7422a1ed30862d77440d0c4e2cf4a3dd059527ff45174
SHA512	3cc85e53656a0b439802c3a7ca31b739d24ef721a07e0abc357ca8a6a65b28f704b8cdeb4dc86174367454bfa883318b87f4c48500b9944b216377956c9c0ce7

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

MD5	5f55456ac1cf41c92e5acdd3c1c50e67
SHA1	658175573828a367fd7740c9a29176d8fb69398c
SHA256	e0c8338db699b510898fbfebdfc3a416557ff63d285a50a09d64bdd4ef855dab
SHA512	5714238ddedfb0dfd282911de7d8dc54dbac54e804e2c970f327391f16b09b1534d54065f5017ce9c8edc120f3ceacd167e572a7d4a4257c5bd30003e72ee5e1

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries

MD5	20d4b8fa017a12a108c87f540836e250
SHA1	1ac617fac131262b6d3ce1f52f5907e31d5f6f00
SHA256	6028bd681dbf11a0a58dde8a0cd884115c04caa59d080ba51bde1b086ce0079d
SHA512	507b2b8a8a168ff8f2bdafa5d9d341c44501a5f17d9f63f3d43bd586bc9e8ae33221887869fa86f845b7d067cb7d2a7009efd71dda36e03a40a74fee04b86856

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

MD5	9f3a0bb96944e82fa8b970300d08f6af
SHA1	c864e1cc4c40628de0011b00b3a04dcd7657f561
SHA256	91fe373138bc81abc9fa7940d0f9f321a913bd564513e63e4ac3a3d66acad723
SHA512	ff90da68d0eff65dbe8eb8814741ea16b23c2f3e63bb680b983964d2c5f5c8644d09d2516ee88732c0e83407beb4d02479a5d290b2373cb5f838a7560acc3c73

C:\Users\Admin\Downloads\WhatsApp Installer.exe

MD5	58bd821bf993af447421d0a143fde869
SHA1	88f6b4fad3a81718edd32098b01c5df02ae432fe
SHA256	df9c66962aee240cfad84b58c7846ce1e010789712c606b5db00511b399ab78b
SHA512	da52c56afc2e42e95b02d0e75daa051566d12146f59313c38f90d1f0e3a5f1da3cd13dd02d5a9d970e79e918112d3d89d708b63e8e2edbf5deb39da847f88182

C:\Users\Admin\Downloads\WhatsApp Installer.exe:Zone.Identifier

MD5	cb5abcbb271b7964ebf7679ddb729871
SHA1	f22e422946a570931c2b23ff2184859b89898dd7
SHA256	e4952ff0cb3e37e22753a1e22be03d635b5de24b3e08c422a2b7e3f7c09b033b
SHA512	abe6263f71802829a2b009bce85904cd6dc0fed8471ebc6a23f190c072bc5bc5c6a8e5ba8630bde1eadf647220c59a0bfc15fc16bce98ef1409b3d64fb044644

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

MD5	584c44260017ca50d8e02e2c6955fe7e
SHA1	feaf20bf9437370d7d76621ae1710a5de46f2299
SHA256	f09c91be3174e3064792160fd6c8a135089f1fe792fb87d7ffe35845dae27c2f
SHA512	81338942fd8bdfede279009552e9dcb7bdb66427027f6deb002ef56d589739a7943182bd4a71d2e2d0886c4bdd81c64e72acf8d7758bc8a7e490a6dfb8b73a18

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index~RFe58a265.TMP

MD5	f6e8ba480fc5646b336d439389c1cb86
SHA1	9683027913dffb6aa6bb127aeb9db6b763445a8b
SHA256	e0cfcc01a22c4133c3e828bc0b2ce9a51174c5a57a2059f86270d433a92a77cf
SHA512	c90271dc1609facdf336e2e96d4c6b867f3848d157910836c46965af5bf3a50e652a8d023970f5cb609772aa6735055e03b5ca9011870b794e4846dd055d85a3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\04ac9e3f-d694-4d6d-8b23-67be8bf1993b\index-dir\the-real-index

MD5	e230129a94330df4601e804fd39475ae
SHA1	e4310d043ac1a95166482caa4c06595d847006d0
SHA256	a5651dffd9d8f80d4c799590a002a9ee59c487156e465d3a5d51b7dbf7d491c0
SHA512	20521eedbac5450eaba781a465b108e40b208377cdb984e4b2770b993fa57d1930d084bd87dfd43afd508793fcf6551c99cc2659552b274a49dde08634cde395

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\04ac9e3f-d694-4d6d-8b23-67be8bf1993b\index-dir\the-real-index~RFe58a43a.TMP

MD5	16ef3a36bceea42d3efbeb941e704d70
SHA1	a65b9ac34cb8f226fbf94afa663a6ddf7f4970f6
SHA256	83ce2b6971a167ccf2a8f4b28d661d3c48338c7928b3c86f5e47e0012d97d77b
SHA512	95904aa5259d09188cd6bef4aeae8bd4c771c1dd60d7532da0d869694ac4e354b581f9d8a22b72444ce025188104a40694a45f33fd87c7299bede675d9989adc

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

MD5	10f517468ccb8015ba4cb686c812bee5
SHA1	281ef05a29deac3fb1ccbe3711f9a50c996ca0f2
SHA256	509af217fd1dd7a57426d2b84dc99f580a72b0f02ec092411e6c16703f82c52d
SHA512	fb7b06aa437b327ad51e3e10bee9a2ccf0c1dec5056e104d1a0eeafa6dbc778e6922de5a52f040683ba6b27b34c80218af77ad409914517a36126a2cf5bff3fb

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

MD5	8d8db43d18bed817197fb277addf85bc
SHA1	b7b55e80be6f042029b627cfbd1a8c1707fd04ca
SHA256	6b0e5477d72b1fc59004e9b98e7f99708f0da402196a5507f31658e2abc43dc1
SHA512	375e3b98ab4f25cae885455fbfaa8865459ada46d04126eb14061e73c88839a438170e1b380bec7982a8068a30ed6ed798d8df46e045d43221fcf2773deaa9e6

memory/3936-767-0x000001D813C30000-0x000001D813C3C000-memory.dmp

memory/3936-768-0x000001D815570000-0x000001D815582000-memory.dmp

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\index-dir\the-real-index

MD5	1454942395f73f72bbc09ab569711d84
SHA1	1a533a004f6fdd13e0cc6efc5695a851d3c4315f
SHA256	e338f8ee0b10f78bed7d29f7fbfcc754154fef72d94fb10559d40056c12a5d69
SHA512	ac2a9e346791af16826817170e54e0a7425a566b8611a87646ee331732da8db53ffcbec20d52d1c6f20b5b8c47ffd180fd0e033b2640757642aeacc8838a8630

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\index-dir\the-real-index~RFe58bd31.TMP

MD5	f9630b0b0e8e845f11a35682d6d7821e
SHA1	9f1e937766f8e6a211156a915fed70f2189db29c
SHA256	4f9364390db74d190d5df9b481a114411864747971f367b12593faebef3eca2b
SHA512	5e7f607fe5406c9cf0949a77ce1b539725dc3e4f1b04e5cf70d1a47c8b89641ebf17ddebdf7fb0460663c5a2cef9162163b5b36c52556331b1200154a62c0d7b

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

MD5	1fa20227857fec7f26ca66b79ed7cce8
SHA1	ff935a41960f3b6a35f1c5bce494e742cd50f260
SHA256	7a3a01f3c8b6f95f928b9ddd02b2e8c43afdbe3a968aa0ea35944179bc90bbae
SHA512	cf45962769608dff5878b46dfa29bc625928ec40816859c40fbd4eae0773411651a0ff658c93066b999066fd358b09fd8dd8021eafe8342cc6707bb0c3258355

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\72ebaee2-a424-47e1-be23-992ab157e361\index

MD5	54cb446f628b2ea4a5bce5769910512e
SHA1	c27ca848427fe87f5cf4d0e0e3cd57151b0d820d
SHA256	fbcfe23a2ecb82b7100c50811691dde0a33aa3da8d176be9882a9db485dc0f2d
SHA512	8f6ed2e91aed9bd415789b1dbe591e7eab29f3f1b48fdfa5e864d7bf4ae554acc5d82b4097a770dabc228523253623e4296c5023cf48252e1b94382c43123cb0

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

MD5	586801b98d19ea38f516d664c91d2c1f
SHA1	e5cf455f39ef3f19b567a1ae639c9b2656e123e1
SHA256	45e1160aa881514fa3d2a75b439d2e94f3c97aad6c474b131fd7698a1bc8ef72
SHA512	5dadec1de28b5d8ea88c9a5738e199cde9e6ae36c51a83e870c7a9d8f9cdeef2cf2777901c47d7a183c06e5faf889b1b3ea4053bb22a98cd4b843dc07f1ac26e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_apps.microsoft.com_0.indexeddb.leveldb\MANIFEST-000001

MD5	3fd11ff447c1ee23538dc4d9724427a3
SHA1	1335e6f71cc4e3cf7025233523b4760f8893e9c9
SHA256	720a78803b84cbcc8eb204d5cf8ea6ee2f693be0ab2124ddf2b81455de02a3ed
SHA512	10a3bd3813014eb6f8c2993182e1fa382d745372f8921519e1d25f70d76f08640e84cb8d0b554ccd329a6b4e6de6872328650fefa91f98c3c0cfc204899ee824

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

MD5	4493c57fd57fad4dcbd66318093353ba
SHA1	8da2678d7e5c0cf8e02b45b3e3ff13e962e011c6
SHA256	1d99366cab140fc11fe7d8a9942dba95ee4927c0a582fbfcb0691c8331450381
SHA512	bb874e14994dd48662f3a3293cedd7bbe0d335b7a7cf3d7ac7833f1dee7128be717186a06c213670d0274c19d835e922c663780d300c8617bd41cfd715588116

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_apps.microsoft.com_0.indexeddb.leveldb\000003.log

MD5	1eba9005e582d4a3f20be296150b34b1
SHA1	80fed633d6c3ffae428b6a6ec78e19f59d12bf24
SHA256	e59cf6949e7f6ae043b6043b6646da2235808e1756eb5dd4b467695b9832beac
SHA512	a93774d2d476ddb21ad1d8ff10d560b290e0cef27e15b6f20265cea85bc7eaa888a6a143a90be210d6c5d90121833477f322a0264351275d54260c573443e68f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_apps.microsoft.com_0.indexeddb.leveldb\LOG

MD5	d9094240cac7a07e5f8fc8fb751aa198
SHA1	0140109d59932407af79882d33b194077a3a5d1a
SHA256	d3f86c9cf0aa7b48e0310f130cda68c5f562b0c1cf5d934cb26782d5eab4562f
SHA512	f89a9497bd3a7e660c24fd0e22df3451ff50788f3389b5aed13dab43540fd7fded741ba118f05263fb1102573e4967db39059f6f5b23b09e4d8a37f27d0b06e4

C:\Users\Admin\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\WhatsApp Installer.exe.log

MD5	c555100ea9639cf3686d583407192892
SHA1	d6552b38a13829fbf29d639ec444448bc53cbeeb
SHA256	641b26004e8d21d44837b1e8bc38a1b8dd021fdfde5ac8dae4f44c0f1971d3e7
SHA512	b48ac7e255c41e57fa42e25d36b5cbdc3a3e5ec1f23efda2c28a0ffb9547a008ca20d3619e5036706d923d97852fec10b620e52de35a3204e24bfbbc8db6014d

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

MD5	b16bd3340a2e33d927c4974c846bb234
SHA1	683f0948f1955613e34a32c536000b3b5b3365d3
SHA256	56d5ab75f536d23bf04316245d8da97650ead0c6144c2f7b0db8eb8591c9f710
SHA512	6a5f1bedf3e9a99bc11304c332ac8efa6cda3c5e73fbbd81e54f6ee81b1a6eec038033a9a11caec2c09710e4f7d8d54b9cf52b5bb4f40d2b46e39907f6d0a29c

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

MD5	cc3c458d8113b8e05cc4227d31f280bc
SHA1	a33352ae1693083ddd46d4523c21b79dcdd54b9c
SHA256	9faa0b7f17e15bd3cac667c528e780433e960748834295abd5c504aff86deb74
SHA512	f41922df6d0a2f8df71d8f10610db3d43356041afc5f4e4626b12993ecb1968b614efc199bd722caa7fcc41e4f6531ff60bc02ccbf811d32465e9952c1a12a4e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\72ebaee2-a424-47e1-be23-992ab157e361\index-dir\the-real-index

MD5	e5c33dbcca01ffff94cc946b85df6119
SHA1	83cbbf4b9b2a9af6b0c482c579cb65aed3862b51
SHA256	ca8b845e07c59ecbc49af044c9bc41c9e956da4ca5259f19a45df89f8d00066b
SHA512	832b2b19cf6fff435d3611efeff1c0d3d5689f6a19fa15fde6fd0d47e1273311e84aad23c4c7bae74b022be0395692dc255fd2a20d1c0d328b9c4a8f1c3f5ba2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\72ebaee2-a424-47e1-be23-992ab157e361\index-dir\the-real-index~RFe590c89.TMP

MD5	b82f1c8904c70f44cdcd99900bb4d724
SHA1	d4fbc5f9b07449639c68b8f85e98cc49300ed310
SHA256	15a635277c21697d66139894d14736f52cf89a593348b9a58004d0a307bd050f
SHA512	64f1d0eb195c31884c4280076d8a6a52405bfb5f67f1cb553901874a7da9cd4138ba2266868ec741cc9c224af2dbea2c93f3df547e63a351ca6f334d52114057

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\index-dir\temp-index

MD5	8d4adec56a24976ae78b73907838d2cc
SHA1	11fc87364817c64155271a88bf62517dc84404c6
SHA256	bf0151f3dc63b79d3826c7ec159d99837123522952fc4776f63ee05465ee9717
SHA512	7756e653a5a35acc8fef3312a70042a7a7b8b4625874ce7d661c1281f4b4420fd6d07ad18aa2ec9e30d53237ad2f3ba39c0dacf8f1de3ad16c3f751ce99d9a20

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

MD5	a29604ba2d36cc0f981969ea8bfe321e
SHA1	a4d6df928a08dce81e38618c6b51d9dc44855294
SHA256	9ee020b1526fdbd0b75864b4e4df8e2b09e8cfb76d1734dbe36cdcd48d5d3ddb
SHA512	2728f87a57f2f9a9ddf97ecf3c2691097a560d266caa1972d908a34070bf1e57c7247a1e24b320d7be5e2ec4e2919eafd7510dad7ffeeacde6c22c2a7628dd88

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index~RFe590fd5.TMP

MD5	aff3f62685d2ef3217653e9779d0b713
SHA1	5ae670345ee31c9b8576fa86aeb66bc0de53a4ca
SHA256	0e505eb6971f2426193e39c8f327293feb85ae850d92a1d24800c7059b7acd82
SHA512	40fe74e68dc85731dc4620e349409c5badbcd7af03fbdc74ea5c377d9b14ea767ce6951ee091ba1c1036c914d868339063832f068394a99147cfaa32e65f4e5a

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\a89f5693-9c51-470b-8ba2-fc7a0ccf1b6b\index-dir\the-real-index~RFe591013.TMP

MD5	309135dbea0a482480351e647a23b412
SHA1	beb5e052c68f49c1cd07ce4e0ac68991fae5f4c8
SHA256	5f6ed19882d8b9c63e7ce430f1a964247b47901e560a609df30e815e27ce5895
SHA512	5c64c7bf39457289350cba57f015e54defdbe087a116ef02f0e44bd168610bbca1de603a5d59f05c41029c002c31d7fdeb4b6bc1e6fbcbd2b41ca5806aabfb0f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\a89f5693-9c51-470b-8ba2-fc7a0ccf1b6b\index-dir\the-real-index

MD5	8fe0c829ff210e26ff93d9140fd1ba95
SHA1	3454a242ef9d3f2c2879a20e064706b8b71aa241
SHA256	ffa85afc018ebcc94d455f40b925656669d277e5f90af333677386e054dba2ca
SHA512	e486a49d7cc5fcd11fbc11a9360d914e1fa5963dabfa3efb7cf44f69d8a91eb3fcdcc28ebdbbcbb8c120f4c58320a4db059a86400f78504420a1c0fb47a3aa91

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\712e09c4-c281-49f8-950c-0c9b6737b27f\index-dir\the-real-index

MD5	4d183d9d2777f80f9e2683bd3ba41776
SHA1	04dc940b6abcb0e04e65c7c40694fa87efe45e5b
SHA256	2d40ae1444aef347b6967ab6dcadccecece47bea27354ed7f28cefe23f2be956
SHA512	e6cc997b2fee6365afa3a6972c6d2661b33e10b1a699255b56c73dbffca27f1c2335769aaa1cc2bdebfdd0a557ebf92bb194fefefb257d3bdc2efff21d2a85ac

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\712e09c4-c281-49f8-950c-0c9b6737b27f\index-dir\the-real-index~RFe59119a.TMP

MD5	c3bed598fda7f372ff2dbbe4b5a7208b
SHA1	e528487d4119a976cb5973cf8412a51450d5ea2f
SHA256	7df554a8de8a6534358d19026dc78b31a2d1e8a6c2592d8546b0ab21b40bca09
SHA512	eff2ed52c71312155513d6961dddb769a47e3c636d1ddb04a34a26830a78c049fa8223f39c644531ba1f12a1e985141d841fd18304d1ae5d6797ca601a84fc7e

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

MD5	3fc535dc91ebb57b543a4b331ed26dce
SHA1	f4be486d305dcdc41fd3647094934dc787a475b8
SHA256	18fd94d24d9559563e4c18b26224c55338a1a23cda321996ab97fc0f18fe3c99
SHA512	0dec7325cda1806bcdfbe449878bda1b5cdb192089b7122ca6b25ee51d3ed26eccf1ca739937f40fc159fc122bf8b9737eeb36f605aa252fad602c6245408188

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\23a8fe87-617f-4f46-a568-29dc9affefb2\index-dir\the-real-index

MD5	b4b33161a2811afdb61a22353118337e
SHA1	22ead42d2f1f41d8889ebf0f05c1d41f8cf78060
SHA256	b799b0f41ec4d628cb17c8d48bf8d81dc9d57cc8bfef29f845bf553452afa4f3
SHA512	1c048b71db2ddb768e91fa792695b7c94a563206d09737266c42175c911d892270d3933a8603afdde0d7ea00f6469f309b7411bd5c4f2b87dae6d393654975f8

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\23a8fe87-617f-4f46-a568-29dc9affefb2\index-dir\the-real-index~RFe59119a.TMP

MD5	c87d9c4db99732c934c2c5a22d744ea5
SHA1	fab8225f4d11c1603e694cbb0f13e37bb17bd761
SHA256	10128e793c1120f6487268b07bad65598012e595cb2da753b38309353dfa93b6
SHA512	4455e618d755fd0206aab0848384868148da77e768fb54b93067aa61e14b8d160a40c87a4cd3aa3f00e7251596d106b9600effe36a37d922fc2e8c22cb20bb9a

memory/4576-1340-0x00000154E6AA0000-0x00000154E6AB2000-memory.dmp

memory/4576-1339-0x00000154CC850000-0x00000154CC85C000-memory.dmp

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00006f

MD5	4fe43b63c131cd9ae8bb217eb5a044b0
SHA1	f90a02ebdb2c9a9096c0cf0febf992f93a32b1a4
SHA256	402f4e10f1784803f9bbd9cf46ef2048ea877c10ef9a8418a7f36ac435812d0b
SHA512	1d55e65ce1783f9959c0aa5c28f3fce82a477dff28deaaa0e4b11b784eab6c053ac52d7c87705fdbafb64e3671e158e76d1692234d567329d6d859cff3c6b2b6

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00007a

MD5	5f524e20ce61f542125454baf867c47b
SHA1	7e9834fd30dcfd27532ce79165344a438c31d78b
SHA256	c688d3f2135b6b51617a306a0b1a665324402a00a6bceba475881af281503ad9
SHA512	224a6e2961c75be0236140fed3606507bca49eb10cb13f7df2bcfbb3b12ebeced7107de7aa8b2b2bb3fc2aa07cd4f057739735c040ef908381be5bc86e0479b2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\35d7de03efe1aac5_0

MD5	fcc041888b7c80647aeac7da338457b6
SHA1	8e4e03db2ae9e71d653cb6feccde29834aa90cd9
SHA256	6d8bde7caa9537e868d2fe78e46b714e4f593555ab67e9bb91e1ecf8d5721d66
SHA512	6f25503e4e22272f2bcbfaeac25ef4f24ea69a1dad5871afccf682d20a316e23b3c43a2559477b109065bba18e15cfe1cf76888d183b0cd6ef56fc6a724e20e5

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\6374f5018a1c487f_0

MD5	93dd94615f5a4b635f3f691a6b22de29
SHA1	dd0e817863951fc223f49e5e581e36bcb4cb7c51
SHA256	ddcc39a3a3d36de482655af68f55b67329de024d72f9ba0845835a2c6d79be9e
SHA512	5266517a27575d1b0b1cdf68c892f74ab0fe3c7d914d1c0054b41b6f9659ea4201a9ff58a16b86e65dcc5ffe9c7bef81145b4af45bb73d78d0aaf03c78f2f2d0

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\3840866d9a71045c_0

MD5	7514a7430f5484cbee77e21e71314e22
SHA1	96ae28fd369fdbf828fe139dc641874299b83727
SHA256	8c6f57e88b7f58afcc0ecdce20061d97dc34dc7bd70e5cbdc9d9e818cf9c4b4c
SHA512	7bf46a5aa0c8d23c94f7033e16ed9d5e2385c1c6902f53c2925b207712b88f303a5bd45b65de60fa8fce225b97a9ce5b69cf7be8450958311dca0dbcd56b23d4

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\52d1c21de945c7b4_0

MD5	f0caace933ba3e8ba096531cfc863e90
SHA1	c3c927be79906fa4f6df3aa78d54392ff12a014d
SHA256	81f3bf575c9fadf13ff29ba825eafef7823c9becd65061492ae941d7b8ea65c1
SHA512	4e4e135baa11b82ec4bd559be2753f1a0175f4836502ed7958c7ca12c549aad5fe697ed37cd246898b0db7626f976f4ff38d43dbc5fec981d587a7263b82af6c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\e4bf23903ceb74d3_0

MD5	b3592cd47068b5b7e63b4eefcd84e89f
SHA1	8762fb4a3ff6084bdb492e8c8ce2cb7b128a4b1a
SHA256	1c683a4da57001fc44e3a1633a240351cb96c1164b3a00ad15edcb2b90bca2e4
SHA512	6c8ae830bc9e314a8e12c19f1c6e7ab709a7caaf24dd7f793df6f586e1be526e7c566430da6a44c1ab23ef6855ceb8d5b6ccb0c7f51ddf78d8017523680e72e3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\18b3a97cd76cb775_0

MD5	1fd3139c926e54c7f122542090a3b6fb
SHA1	20befbd142156696f12e7ed6293bf6648d89de61
SHA256	ef5d86dee9c6133b87e37ee5140a63dabb8504426204526487db83a2489cb479
SHA512	f42456c4fd391a727ef3f3dbdd10e876ae90f8fd408f52724f0060ff383fdd00d82bcdeb1a6ab296ba1c0aa9a29bdb6ed286f72a223f23f43eb605e8e4f0cfbf

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\a3ca9584d9501f0b_0

MD5	4d93266d8162ccf11b0c4a071940e6e3
SHA1	45e9172dbbf30ca6debb999baf88735f41088d34
SHA256	1608a26aa8e3c015f4ef592d1050a1fd2ff7387571f31c8ee989948869e5adc0
SHA512	7fb45086a744e601f09746ce871819934fc0913de4fb04b03597a297eb69f8b282d1204daed961e5dc1b74900b7e768467637834d954b61703bf18c402d301e9

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\cbf7872280c33918_0

MD5	38ef4affefb78294785cb920ef2659d9
SHA1	2249842d9c7e0eac551ebffbc8e75f662190e831
SHA256	58ee36adeabf7f71cc021a1b30926dd8f29f691ce02be7484dc3e097281fea97
SHA512	d385989c3b21af539fe80dfc28c774215e59c339b0ddafd83b4fa8de28d48c1604bceaac12526d3e80eab69ed3731fdb62f325675000af77452f0c8089b2651a

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\e74c51c735ca2941_0

MD5	b376b9f0848c1ba4ac09a185db267541
SHA1	3db649b2137af0c927798da3551c055c5c52299d
SHA256	4f95555c52032c5d092e6d90925b69ea9fb7107f96ab5227948e018afcbb2c1f
SHA512	5e77ce38612da2f5b7dff8d421a7851de3f78885e8ee7f01e4d0ac38cd5579a2b2d027eb2867a6b895dcfd42679711e5ede420a8691867c01c2153205527c167

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\8fcbef4f0d543237_0

MD5	8ef019bb9db6f1628cd535ab2b6e76b3
SHA1	95a29ff3faa8f3aecb472d8d4e26daa1e9f5b0c5
SHA256	40424363f61081f1758d6063aac703b1cc4adf91219a2f101ddff9a5ebc32272
SHA512	fdf2c8f7b42913d92c85645939e2e2ab40f481e2c5daa7b363aab8f575c6f171418687526a0dada181c3e95bc638f6b51bfe6c80a09db067bc0b9d2d00a05c4a

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\450390e75b047be9_0

MD5	73814491db104610b30e4534252426ce
SHA1	3ca7b31e95e01db25f89f1fe2d9b59b9f65b4be4
SHA256	c7670c748ebc0780b71d50c75bb0f765cc58cbf76e37a78b64cf74a010a8c66f
SHA512	1b99894adad25f1892a89ebc3d5746e10898e1cdc26a008f0591f22e1b60f6fb90f64b06644ed205730d935d40f461d1085f859e7e413d89fdcc53b1f09e05d1

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\fed4a131d03df326_0

MD5	1e14de2c544de7a8575651984223c13c
SHA1	c30dab992f4929659275c2b423ad4ab0419c2aea
SHA256	9f9e53b80fa07a985ad08dfda511afff66f18a99476fb06b619bb9187276461c
SHA512	310e17f1261dc641dd38b06d21489ee4c6252f11ef5d5478efc4f0f6cb6eda510c1bcc65fd7a630a0bbc279c796c851c94dbe6653640aa83b99829f1f436ec78

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\97e4757b53291d61_0

MD5	3ff39fbe93582253ba1e0b23004fb367
SHA1	23ccf012ad650de52df3f5681ac302e24695fbd9
SHA256	c322d6f204ac22ddd7f11449f1d783644044aa95ff2662da3fe74431c3808b25
SHA512	1f372c2a451799810b63b648c665c0cf324c67ba5a2bbf9bfb22e9048b7954a2f823c5db0ff83a7851c80e2602fdfae6e70d1bf1b641e478ca55571a306e5517

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\75c5bed2d1c49e80_0

MD5	2c5d4e618a4690e58cd52772c89b6198
SHA1	9aa2a458482b60a9a890fd3b215d8b3127b912dd
SHA256	dc34920044cc1b4220e90cef96b0adb07a23ff2cced7fd9b500b43bc898daffa
SHA512	db0e2c9a867c18289cd8da1e5ebff56aae7d772d285014ee16815fa5f411ec760057bf2e27237e06283624f60ae6e1e6f5bd5424e1757d1524909edf9bd448ec

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\3994225f47dcbc94_0

MD5	7106ba03a0deb30d7da4edf8874fb33b
SHA1	e96da32fc5afcadc4af668fff7e8873c0012e38a
SHA256	aa43b44b562b1113b65983e9a15c2f9bc9eba9939ec8e96754e2c6c99d5d0676
SHA512	d78182e30f044cb50e419d8450bad99cac24821a55004dcb642a0c3339b30f0ec1f3fc5cb78e886a9aa90d6bf15de829693910ee03c006c7014a94020f748d98

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\bbee7de0a6f7bf6d_0

MD5	ce1266000c1c9d1290db60ca5d14d860
SHA1	d921e09702df2d1dfaee274a30f0dac768dabb0d
SHA256	8ee766b156e5829e58696191edda1a7f9ab76658888ab6a08e90332ec262e5b8
SHA512	2eefb123a1cf8343c17da587607161fb74f19e27615fca5e1018e253b8b19722cb1eeee16d305fed039174ccef3064b3983b7ba17fbb127f3359faddee2a322d

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\9c0c8298b7e5f370_0

MD5	3406bdd0b479977748396fc3408ca72f
SHA1	40797d78a8fea426f153a38bce7398222fd7e298
SHA256	2ce753ac14af73abfdca25c399a8e20b8fe1145d3c7d9217fa129ab91f8826f8
SHA512	aebbbada3d8f31cbd49eb6bc899d8a03b3b0a9d9094337b592b416c81839ad3058e9f3d74fd03dca8c805e662a2bf8107928530d79fc1afa960dc8cf0ce7b263

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\caeca068500d375f_0

MD5	f9d77b934e62e13674c3642d7b89a03f
SHA1	621cd41bee9689bedbeef9f743fbb3a9ea7e6376
SHA256	f919f2101a6b5be8bdb58399a32510b7d0f1d477905e7b0584a5a159b431ccb8
SHA512	d5f703a9cd0de38aa01c650e12027379b76f28de9865d838758a60db87771e20a175b33224f8a8435c7bb20a0b6f1078a7a21fce924c85ae2c5ef2795f4d52f4

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\5baa3065d51b38cf_0

MD5	356df98fdadb34fc56c3dbe6d46a7ac5
SHA1	38ea9ae88c8f60429ad517491af45a7e8e544534
SHA256	765eaa1eaa91831ca00054e4e90f517335547419b53eb9b9c001043eb2aef7d8
SHA512	1b231e2d781df6cfe2ed8378707fc18371711fa7ca54e33b0a5de7f51af82d2caabf0aa05c2d574151424bba004ba87cefc837a9f39120051fc5881a39523937

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\44b57cd31d7ea95a_0

MD5	cbdb7bd36a45c2eb51d08d9a22716cfc
SHA1	84531f4c5a4303d7aa860c6c29aa0d597fb91abb
SHA256	fdbbb007df6745819f4768efe8169404f49dde0c714d725d445f3e392de52a08
SHA512	4fa4d6e0f03f81cdaebe6af0e6ad5175f5653d7628297b38166f58406417769d04e62af9ea6347a8b4488c31d61d6cc09a4b528122bb303d9d1c9f324a8e6c1b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\1e4d4d52499a2e02_0

MD5	c82bc56be5e64565bbf2a54d4847bd6b
SHA1	273a45786804bdd2e9f6bf2e7342b4e0010beed6
SHA256	5bdf061cc8d24e5637c136050e5eff75dcb938cee42bee77f431cebe4310e403
SHA512	589e41d7c35811a6cd8c8640fc2e4e93b8f2f942e733f7ee805cd8e94f5c853788ca5d291f31b3e321665c89de882125c49a3ca8711297cb1e7a830e7461cc16

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\0ab68bc4dbcd9b8d_0

MD5	7a6fa68eae582a959e27476f58c0ce1d
SHA1	1aeb97e5f0f991f2d106165488467aee4a7018a5
SHA256	831ba8c3263b1c3fdcf37d2f851e820a810d0b8132affa46f56d924f7f827de9
SHA512	a11e3ddc76d2ea6b0d0e276fe2335abed5a509c4795723161c433040dfe94a7b38dec4dc4638822ce1f0420e5429fccfb2d108fc547ae968c5543fb5bdbb0e62

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\4510741152987ee2_0

MD5	1546290a98e04524e475046442bcd358
SHA1	76c55e74b8d6146e2fbfd437928c0e34f38c87b0
SHA256	89d3473ed47fbe6bc8cc515de79bca76fcb67988143820204bac6a8291765dbe
SHA512	5cdd1f33d1bb9392e8d44283c72daef0e990a969c91f777485b4af5f06d7e9f554db72e110333b7f0a572f1938678b8cdb05031be98af1f3fb0b56692b85ea7f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\df3bacd705124aaa_0

MD5	adda9fc2a27782b427cc61df8a2bd0d0
SHA1	a4ed87da7ea0d87934b59131e99c1b4e2ae29dd7
SHA256	268b96838cb2093c116215aebf371c6753af05e754ddec622a518165c352020b
SHA512	73f24f76dc3b217ddd3e85bdd1a90a882db3dd1a368648894f43723ddab441e678ff9bc6171dc7c65f34c722d5053de56f8e521e57e87fb1515f17125f6f45c1

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\eedfbfc23566c8be_0

MD5	8bbcb403540401362671ef08ce214441
SHA1	7cfa2d3db584290d8af4b8e56cdf25e5968095f5
SHA256	378218eadae5fd430bb8131d46ad13987c0d9ca9a0589810aa4dd46bcb4bc8ed
SHA512	a7e959880d52c2bf0feaf12bd1dea4c02cf4a19fd0d909c4363478fab88af8fd4cc3f5d700abecd376e02fee20535120c0611867afc0d66268fd7fc2814645ad

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\7557bfa0af92ad4c_0

MD5	e7b6e0944a3b4c98de00ec091c1669df
SHA1	06e0308b9eb5e2a665585f00cdb565a994387030
SHA256	c209bb2fe481483a0b66f5f7463fb14b8bc3481ace43d166c873547ac0d70024
SHA512	53167da6ebb42fd59314bd71eb3830827827c3d01b477257560b1157215b1ffe25676785d6f6fd09ca1e604e3710be4e14aa5dbb890bb38f50d17be8c052cec7

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\2653a8f84709228a_0

MD5	6ec5246666539902f3ec8798d5d0666ff
SHA1	0c57a5814ee17332c32f23f472c35c02d0ef0753
SHA256	cb576f68e6f640cd384a5d649f471453e6d59e7215e3ad7bed7d5150266b981d
SHA512	9b8356d58033a753118fbc408cbf8072297d6b73305364faa191657be020e56b01f75561763cb9d307d023c887eeb7507333718d5b090d11ebe813e175e85347

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\3e1edd62cb2921b7_0

MD5	469d47ebe53dbfafa188eadf6af74f55
SHA1	6df46bc69ce6c396f53e9f40c53f8d5ed3f78ad9
SHA256	25a398e641109ead7f97e142c22564e9f0caef194f5c5d8f26f768701445de35
SHA512	bbe645dbc2d92194329ff0c895d6614d4a38c74a564a9891cd2c876018fe1b17ba4ec3b96790fbb0d32bf7ce6e7450f04161aeadc0a4f662bba17f692d3f0bf1

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000074

MD5	976a6b7f5c83ed356e701de35f6924bd
SHA1	df26da418e5348fece2eb0fe4feb21f1e798df30
SHA256	1d84fbe673a2a518413576ab116e4fd8592c08168ed7759ad23fd38cddfb10b0
SHA512	c39ba71964cfc6e018401e59630605b3abf66d8c68a610e6ee857c5c3a8307628ebde3efe273491dc60e1fed35919f463addd20eb2d415498531f26930569e50

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000073

MD5	146c72c8d8038056b2bdaf4fb4b12a5d
SHA1	a21bddcfc5d411d80e5562cc86904a561b5d4cf6
SHA256	a2331594e2efbfc7d70757fff5d4db9772b95ef91a6558ba636cc6d385e92801
SHA512	d55f8ee251d98fb2648eab957e9060c6772f9a45b390fdedc788b6d9c5aed290f2cf3508e06cb059b1d6f0f5284ed95d0d231e05768d48b0e943df9815b84316

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\79dd15cd46aec099_0

MD5	46cca64983344188877372343a57525f
SHA1	04701467dae4d7ccbd2a4e74fbad7de19061ff58
SHA256	e07706d327b92c1b0ca624e57f8f44b20f6a10c024f2c38a8ee0820552f3d87b
SHA512	a89c2135139906cd5877941c41ce7fcc642cad6cadf12c2a8313ea00940feb262e06457d10c5accf2e9c460f47971e12492fd4c1a85fd6c0d887d0425530a8fb

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\1427e9d5432c73cd_0

MD5	88e704baebbe8075e3a502295da5fd25
SHA1	516636ff422cfd677aeee60deaae85fbf276fe78
SHA256	7d0a17f92b9e871312421352a2d2434f31c48d6c4dbcc1639fb7e512bb8746c4
SHA512	042c9965951eb2b1670fe4f786fb3480d6960b1d614a104b2abbcacee7227bdf860ee4f85f26c4e18ee29d161040035c7d155a6b33ab67dff37bc6aa8cb220e0

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\af04585b800b7b2c_0

MD5	927d7b53a939f315103ec832d3112241
SHA1	1aaaced17fd5e696cea1b3394ef868a34a416a3a
SHA256	5acb6b5ceb51230a82c849e428341bea93ffa30c64134698e36c01c6c5f244eb
SHA512	79b4ee2455c8f900e550c5fe39adc83455c1641957f211083df95913c3a445eb0e19b7e7cbc6813e8620144a5d15add6533bed5a36d09b9907523df2b860032a

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\eb5bdb0083767553_0

MD5	aee4cd5a6a855b48a6de834bbd794317
SHA1	3a06758162a5ecc3372eabc363cca4a464badd5b
SHA256	5ac78fe80cc4626a3bd7b5724da2a5c3a3ec995b82f1ecd189a160672b8a526a
SHA512	35b35bc48829216f4380050e269aaf52e2f4201063fcfcfc38035b408b64809bedbd2e0594d8bd9a7a24544c98cb321c3b02da726dd10f9c4944f7c09e669330

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\04b91793ef6d3705_0

MD5	77764b8328f5fb79f6f05fff002985f7
SHA1	a3e538d04a4dfca195d136f1f471a45ce88dc63f
SHA256	bb4775b539803d63677988abba36ca434d963873c07e10ba129d2e1661c4f087
SHA512	3f60daed1285b9a3a32e08772ebcd8b7b398518670b0aab3ac50cec215a88d8eaefeb99c3de2388cb2a5d240b6da5c870c42a7f2074f71792debbdf17849085b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\982f44b4c3aae948_0

MD5	c32cacd86754246e7c2d7787aee60b4d
SHA1	fccfecb98cfe803841819c5954865d0d4cc04200
SHA256	52b8ed901c5ea4e72650862480c6d38b5261bc98330fd472429980f5cbcfa817
SHA512	8ae63fee5c075ff476594cb91387988572d5cc0a6f8b876a9ba2daf49945c90706c628950919a7fd8316919a2d00b60fc19e22f8bb54bd1afe9014d1bd404b82

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\cee84ff6c2af03d8_0

MD5	8dbd56cace2c78e21bb62f37422b7c9d
SHA1	87e39da3b1e062b0d7e7c40980c2f1ed103a1618
SHA256	c0b667beaa8a5e7c5282b5dedf00d71eebfe69fd63ce07cc645b2df590cf5a82
SHA512	f9954fbb01c8825bfde6b9028b171955927654db2ced4dcb523f5105223a209d61a1c665acfa611f1cc937dca12992583f2c74c29b9815c295ddec4ba87def43

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\60a31db01f262e1f_0

MD5	29aa664bd0146c6cb8e0190900177684
SHA1	fb7a9813ea2e70dbe3533d2f01c15d12211898a5
SHA256	bf014ac558bf317de11ad0fe69f6ab4207fd0b28570d7e5bd16dc384b3d03d78
SHA512	ff2220045b8bca562ebefab57e9162c70ee162cb44ae524f6c211d647405e6f7b9e58f5312a3710c2b2c0c1bcaffcc7c9786983e64b7e60c68c7e2c58c7fcf41

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\4d249fb91a931d36_0

MD5	e01eacb39480cf72c703d212bb0c8780
SHA1	a53a9dbd70fe13c646da7c8b0e67fa42ac73c2b0
SHA256	434323f35937f9f0d4d4b6625fa4666c95f968e8438180e9d55f1f8a8a08fdc6
SHA512	b0a90ede1f01fd4bad8fdb5d77f2607f4b03c255fa52f58212eb05865855e5f07313b80ac448fb9b333aad6cbc630af27388aafb65d1cf7105d47b314ae43236

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\4d3d40b46ae35c4e_0

MD5	aa46a74ae96ba69ddddf706d5257926a
SHA1	ab7737ebbac547742fb7bce5b102f388239cdd34
SHA256	7b6657e67a842a8aa5ddc984324d54e0c3933911de0a582514c081e7d1b3cd12
SHA512	e41db5c560dcd1c270410d42c4833461639d4b85c62174e4db24a7c63056959ef6ed7fed739a621026d49d5f258971d54e7e69c6bb2b8b08b65a15de34e3b005

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\7ef52e2296df83c4_0

MD5	d1f55b72544c048df67de9f820a31420
SHA1	a9b413600f3d4cfdb4e61f307872fd3d63ac8973
SHA256	1c385ca8a2513351ce617bf97f1cefe56c218576f9af7be38ac0a76d70399ea1
SHA512	6f55f4cf868633a934683caad7497c293d2b3a8af9ddad2b25c2e92d68f10842989900abdba35ee3d02d435085d91f8a7452c7a78f71f4c9c4854899906e6986

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\67af7516e6dd56aa_0

MD5	a00c6a5cd4bfb8c107bf4126a77b1268
SHA1	cc6e59e5c2b0416612da1a7442313546481210a8
SHA256	e6b43a279449dfdf44984fd53e2b0be0c1c6a665c162efa8b548b6974c58a7ee
SHA512	b18003791a029507a44312a02a8762090b70a036fadfcc69fe768e06c488f8ad50c82ba812585548bddd4880f81171c8677247344f48360cb4cb50fcc1ca0dd2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\3b6f116a1aed8a25_0

MD5	709cc64cd7eb9164d51965c2dce51404
SHA1	1c97cf2ef1edffa46f8b768377694f5677e574dd
SHA256	580a8d781ce09ac60ba418de158b8067387e7fb756f7eaeaaf1f6a5f2903717c
SHA512	a3d1615bdac19c3b9ee4f49253cb755b615c4abb98fcc2b5af8ab377e572775b08f5bc69d2c18f59cc80b009902264add6b4c1e7940a271bc2169b44aeba5c82

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\5a210b81ae128e0c_0

MD5	0abc16d3c8e9d5f18920859e9fca057f
SHA1	a1f7cd651c1c9fda67ecaf64c809ee600239eb47
SHA256	a2781c9650ab3634f84b5cb9cfb0ee4269d06fdf534d26c7cbb93dcff769a4f7
SHA512	98d6358b52ea451acc1ec94faa49f877c0e0c8c6c5dc40aaa0c831d8706a7e2c5974693649490d76f170cbd3f22fb2be16558fed6261d5e786de24c1a5fc3dc2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\1f10eca99a4d4a16_0

MD5	df37912210a9c23d8cff67334900278e
SHA1	7b78f39788c125c72b8eee636bae2a590b62adce
SHA256	9bbe23e01513c5909fa2237fe2628f16f64e52abf35d03352b81672824e17e98
SHA512	2b2c13a8c7d301247f1330621e717638abf7e2c2a2630bb0546a5d2efd5cb3414243d954552de0bb9f2ab24b057e2192fcd5ed7c25d9f664ff7d3359b7f93fee

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\e6a32ae36fe2e210_0

MD5	cfb04f7aa40f838d2cd68009831b73e3
SHA1	85c41c5d6fa2ed0044cace8dc02c8bce4418d5d8
SHA256	62d02caaa2a9ffd1967a51f77f63a5056fca2a4336a75d20e3aba8f3f670dca2
SHA512	51b3928f097291ad9f70c8f5db3726e12ae0a3c53a064b39d1b0660b1688e0a8d538841f623e6db5f9eff651c30a499fee1e0a812d3c86aa5583b6882fb36f8c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\fcce71e589f4932e_0

MD5	b8f5485ac10be9f4a6bce737a5363798
SHA1	d77ad886ba10f0281a562464011859085e056a8a
SHA256	1224d117d26c22b0c9fa10f63e1005d60e53d7b584bc4cb479e289ca9f558d51
SHA512	fe333c6b9be969cb02e6864b1edd7c49588cba147dff5f52edf7a28f3b4bd43417688c12117fdcc185013b265b2cf42001924bbccddca780929b7421b73d91ff

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\6e410153628a49c2_0

MD5	f9b1a35fed4a0826b0486efee249f623
SHA1	cd57179f5d5b0a119f2b146140b4a436f31d094c
SHA256	304d247369fef8d56161b0dcacfc36855bebc209663212261bca0ddfdf4a8b18
SHA512	9739594c991ad59a31e4472db2092f9307f9f2ace4766f6771194ba7c773bd477264e406079b4bc1352164e2d1958ce50ff92a26ae25c2a31fb125aadf8b7e75

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\5958e80ce31653c1_0

MD5	e67b22c011fdd55829d3aa31c8d7a019
SHA1	bc96e175f94f56544ae1757b2e4896361d877753
SHA256	f48733ec2abdd0d566a8238787f05462fce826c9503a01987caea4353a50bc5b
SHA512	4a342d638b1d16e32a5fad324511aba29ee295a5f490367ab4a80a77132453a53b7db754f5a2089e930af543f845f4333f72d32d717661e9a787b10acca4ab9d

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\a6c81192eafc8212_0

MD5	ae7633790064d176b09792b9425bf3de
SHA1	4723ea0a7c67dc0fb9bb972ca26c086c22c4be97
SHA256	39f314817dce4c761f608826e38704b01449fb56ca1da4ae68a9b0d2d49e2176
SHA512	97c3d0afdd0dc11daa726a020e6bab19dadaafda6b7cf132745254ad0310f2430bfd2b2d39540904f102d85a93969f5e7ae329350cd449c4f4971898bb516511

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\b016b99f6947f05a_0

MD5	d84ed3afb3664b8b7071c8bdf5c980ab
SHA1	30fab53d8d43009d6dacaa6377f7bc6bcf6f6e63
SHA256	e16d573f921e4c1f0ef6dc85646ab0d71e0ba3307aef8a96522e7a0f1705be4a
SHA512	e7a7f098b39b4d0d66030c1d4987c8625413aaa5ec0fb7b5b5e2c517cb4f37dd2632ba496fc6bb39ade1c7226a4dc229b7e5490b077c6e72b4652db88217a62e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\36c2b7d96df229ff_0

MD5	6a0a70c2aa5b10834da41f0073590ff6
SHA1	da507835e4a9963d04e86c80d7f1a0e9b761a1ae
SHA256	015159ea57160ecf742c3f0d2a1af39e93257742ad40d754d38ae8e2464969e7
SHA512	95b58fec94e4e35cd302350c5cc393683c6051d43eb9d62662ac5b6ea9a191585907c84dd0d26b7b1e399239803efb8e04bd702fbbcc3a12af81c5634bfc5f33

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\5e14ed4a0954b57f_0

MD5	5962694ac8038f18fac7b4e1d8b0f300
SHA1	afd9fc4aedfb15f20f952be5864baa91664ac6e7
SHA256	108e55ad7819c9664e7993b7bac4409c4dab8cd48b90bbeccc30aee69e80f59b
SHA512	ba8838cf3580582fd981d47ea5b0d377bf4030cd04ddaca4ad07057261d8918f3f39674e27bc3560cda86491bb3f23f64fb6b26e26d07b8f4d00991a880ab1be

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\04e78231d8c87fdc_0

MD5	2e4a905c675330a38ac8c496caf5f377
SHA1	dad1aa52c2ed417863d78abb1297d37830c29feb
SHA256	4c9f2f5765853d589169b8a0901d41825c13522a5ab4b06d122e8f5b9cc0d519
SHA512	24fb41e29a909b0267c364e3082bb9c19af5f0b06b1f5e194a2d0f4194c8c4fce1971daca19117411cf37a7f61c978c035fbdfc47815a652c86aee6bf2a0bf55

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\f7635a80580cd8c7_0

MD5	c87a163e9ea9ffc6e792a43906c00ce6
SHA1	b5bdba54b5a3734c0d53137f80a3c94197614a33
SHA256	acbfff250c1fa82f0d1a15c38708b3a297c56eb8abf15c0f26b5b95eaae0d374
SHA512	751e3a5fcab2560fa22d42d7a1ede75b29d10a8f882a8ebfdcf0a8528cce58206551b17a4434f2259f9bf9be95302f2854f0cd98ab968dca75fdb3d054ed5e39

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000075

MD5	52bc141576ddaab63924fa360922f0f8
SHA1	30b7fa3c71292c41468a432174e203e69bfb34af
SHA256	093502cac263056a82ad4b85b4f9caedf77a7ae7b328420636bb57cfa71d1e0f
SHA512	667d7740613f45ac06f1276f0b275b24bd8a8798061e2d9d6726b774052aa0eed3f31cc89ad2e26ca4f0984699b204c5b9e2a128847e4661641fafc87f591b20

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00007b

MD5	03971a286eefb5c0da87897648a2814f
SHA1	d0eae33dc571db388369803ee896295d695a1bf9
SHA256	7456464773f0b517b5bf1414eaa75df53f0aec217b84566a9dd77946f650979d
SHA512	03bb0b25ab091c5a63b733334a9e9140763759ee0e36036edc6176a9a4335f3b97c0ff74a724c8e0a46b74816d1712814988c848a11e4be31189022c45f3d6ba

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\58ac99cfa5e0d441_0

MD5	959dae13f8c77b9479e808a2c8de69bb
SHA1	228da7a6c77306eaa410cc57f30c7020d35fc4d8
SHA256	fd87da88c404295a7b7b971c2e75d04c6fa128c0393efb4932e498d9e370b06e
SHA512	47d13b98c7f9f596d3508e4bd87ced7b35e645e7b1270998824edfda46e2161195d1a4235772b5c12f3a960c91dc9ce91e2d3c3c1e753a1b351279e6b01c4e38

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\712e09c4-c281-49f8-950c-0c9b6737b27f\todelete_19c4f6624ff8f95b_0_1

MD5	3bc2aebfb9452a1ef0974a658c64049a
SHA1	bd8c3662ba6308fe3e9bde12f20f488bd7d0c498
SHA256	687c08a53a007a0c8d876adfcfeed644866716da7ba2d52eb159b74e941023ea
SHA512	317c96ac72748451696a00aa75e104c3343dd9cfbfecd95e2097616f9f9faa662696cef7a24fd1d660b8b9061cb18a46cdc2ab930623a9ab9b61d1a53d31f315

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\712e09c4-c281-49f8-950c-0c9b6737b27f\todelete_c41e72145b911260_0_1

MD5	3a5369de6e55eb6bd2c7f4f0d608f64c
SHA1	72f4bd149f930777e5079fa00dbdb235088370f3
SHA256	8ea465a4c7b25638f7efa2b38b431682f3fbc1bf83820d0facaf49db2bf74044
SHA512	531ffc7ab3911c45f181da6c8400554e256f138531dbe971493da6d4b9e4d1727e2e5d913d9f62f4d65b7dfb2f412e96c578658f285a9ed6f55a34bf902177a2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00007d

MD5	4e52413a3576c4ee1ef01dd462ab0daf
SHA1	a04ba42f55d5296ea785a16b70fdecae1712197c
SHA256	abe848674d468038a124c9500af678609ee55b4269d2d431c102501d4d810370
SHA512	cdc78d0cb456fd2511adf3c6fc9dec83bb14f9627ac25f5f63ab2a800ecf821049743b82a3fb11654ca8ad8f1e70937b980759d040ef41301e14f11d594bb7e8

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\f0d3fa64ac5e2c1e_0

MD5	8ba7adcf54612697cfdf2dcd69c4ee96
SHA1	2fa7d476bd0d77a827e02ff13cbda0c74629b601
SHA256	2ced9304217e89016997b3f697ec25aa47111e31381f5e47be1769e15bf5341c
SHA512	683fc1c311c72bc1c4ebc3bb22fb95a6569f6bd6b297a8c36ad553733bcf190b40704f7bea423c52ef2fc0721d4ef42f75f726754ec7ae4b5fa4810eae4c881e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\bf74f0351b7d21b8_0

MD5	eeb18ad381a4153ff080523ac5462e66
SHA1	176b3d1494238c598999ef7eae255bc619cea82a
SHA256	fd37a94c7c8d173e625488fd29be9cb7f404dc91b11ee4f54ae8c01d371e5764
SHA512	9149e6e487eeec69a59edc94f0ec8584c1bf2cd9cfd219688dce89ca68280dc4d42f1dd9c7f667aa3c1aa5092fdbde1d88b46347d6345bd3f862d06510ad6508

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\5ce3572b0f17bd65_0

MD5	46962dba3bd7f8d7541d5b49f36d1185
SHA1	a3e0b84b5050e194fc3a8367747efee70d2cbdb6
SHA256	00996689ed565f6c74542c44a090d912ed0a00a47cc6116e1e30df2e09ba06ee
SHA512	a4d3b7efeab5082d7ed01a54decf6787c095f8a2765f670632134c1786eb07e407721bcf7e7abf4401b5dd71119ef98cb291f0221f74ecf6d6b168298fc0f7ae

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\1663003399353080_0

MD5	6a658233c526b31c651912a8f4e24bdc
SHA1	989775f40bbcd0ff355cefb490056cd9e969c4f1
SHA256	dd9ac19fc9200e8e97c13a086006c749b26ddfec19f5d11104e556f987012f20
SHA512	f9bd60d6d9de9aea6589e0eb7c4a055e0e9eb3debe93679c2a25ab101947c29a4f2ab1cb1124b9322f49d608a2f9cf65780b1cb7766b6631d88a4a226fae6137

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\712e09c4-c281-49f8-950c-0c9b6737b27f\887d8bd9741178d4_0

MD5	c1890a31026c78272cc7debcf2153594
SHA1	bf4c008c666593e3680df7c8581b42ce819d48b6
SHA256	a954582084b7009e847454447aa8409ebc0b82f95091283409d344036424689a
SHA512	2c4d60a473a5e2331e1f442c9cf170764968fdef70404f3916d466eb23181cb9e29db7dd5f9d8326d25cabcdbdf6ee96cda241cab60cdcf4fa94b2b8102ac960

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\02411f05ad14540c_0

MD5	2c0fc711eb1acc0032f9ed33b33cc7d2
SHA1	e186d6b120d59d166c0d5b2fb97806d5615c0b94
SHA256	676d72bc613e61f7a387cdb216fcef042c2afa6abe72be4ae6b4eab8122dad67
SHA512	483654c7c536d33e9f79ad44c7bd93dbf6cf894e52cc68a30cd325be86423b76c8f38aeb587e910b09048a7ad33d43c16df13910c74d5b550218b339c28e8989

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\8f1929bd2e8f0a77_0

MD5	2ed8b541fa9b13504b388876a72660ef
SHA1	e78986762bdafc31ec5d27e0e0c6d4efb6378437
SHA256	c665e72704a540406d5b931c39f73682264c654855f9f127446750dd4c1b117d
SHA512	7f6040293edf24b998c0f40be31038d10abd5d29b28bc6827dd0405496a048f92de610aca989b54654d335f50cdd017cceb30288b24356d8066f23f30e9a07d1

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\c5cc4aa392845699_0

MD5	b058f5abbe67f9d1075df67259361e5c
SHA1	aaefa543de131f20d96df0d5a6cc03fc788ee185
SHA256	c3d01d9299f702be4916c603f79c6c74b81ec009251cbbc5312e20a8a9aca8cf
SHA512	a5bab9049a11ca8d8f9277cbec195a8524d20255af195b69084b29e4ebeb1fe081c51b8f1a976dba8cc46a811174c5b231b0c71eb922cc5f288f5b045830da1e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\6445c78e822fb8b4_0

MD5	5ac25ad1f508fd6fe04f25957b9d3e67
SHA1	d295ab9c00b98e4dc77f5cfa4cbce9d0e9b77fed
SHA256	3f702d44c3add4bbe33243dcdac539c1e6c3d66343f824681bf4c57431a29ee9
SHA512	dfdc70a74ea91dacea1ca49cd5d64dac04409df3ef7d2338b1a519b8cae6ccfa84df91635e1960a15c7589dc7dab26a8cf7c45d1f40e0b7b61d05c106bf56b6a

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\8c89540e31f18088_0

MD5	93a0d5bfc8d1b45ebcf077e981dec149
SHA1	574254a057cc44f7d7f22d0ef0460fa68269c49c
SHA256	f87f4eef49255c7e3516bf09ce5db67ae7250cea9ec3221229f28faeb4d94f19
SHA512	65b7e2836c995e8f321b6640e75253469aaba0325ec0894087e78c4f5abd753f71d3f2fbc191c94167dfbea01053bd879b1586f33ad1d7f80a7becab861e77f3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\5ae411b33ae1e117_0

MD5	bd16cc2e65297830894bd031a40f24c7
SHA1	54747ff2eab5f3426b865df55c8a6555b96e63ee
SHA256	284c5374e01d355fe0d54b2ed5f172fc691b5af6a789967b342f827ab3e9b5d3
SHA512	2ddb5195b1b1422b54e78047c6f0f76be1573c73635aee0c7dc1166291144fade211e1ad3ab8d11524649db313f92f5e7898163fa9f41171f476fa47bcfcffe4

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\df4e68eaafb348f5_0

MD5	5a360342af6844e73bd8f24e90f5c755
SHA1	6bcd94c780d309cc3f21933bb0a28fbc02ccb31b
SHA256	c6a06a18684bb9d4483642c04d6f26350c01cc50842cf89c7aee4dc8e11e4fe8
SHA512	1642d1965e84c0d9fa61de8294aa9b51a7dba0f6480597a0c81495d5fdd652f7405308183603efce3128cac6147892ee14e95253d10fd54483638cefc8203b7e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\1f9a356bc99f6540_0

MD5	007d845062dbbe31f6731473085200ee
SHA1	f504c8883064dadf452766dedbe726ec9c39c2b9
SHA256	9ea0b51410516a98191d4585e73a8f607717e3fc7ac55c63f362f4a3b9867cd3
SHA512	d4deb82e60485b0dba9c882579098f1b5c43a25e4bb81892d8422d699800ea911dfe016d908a6e35ebb1332b0d1117b2d6ead1397f100b8a578829c1402a2651

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\14b54641eeb36299_0

MD5	a7b49d15472fd751793b4f294b2c731a
SHA1	e20f3ef14efda1a938de2fe7ebaa3461a8b56e88
SHA256	132baf720eb256caa803eb478df9fa3ef2190a9631e9ceeb1a0c261d4c33ad12
SHA512	fae57d79080d8e1a04b18fed0ecad5c59191ff17245c42b8de25bef17314a7d112f9f2b0c2c59956cb1fed2c35ef0a422556e6e3d20b14aeb269a8c886bfc5e9

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\b4dd29cc69cfa13e_0

MD5	de22a877916b8a69da55f49aaa75d192
SHA1	06169a235def3f163f0a82325806dd89da672118
SHA256	e04b265ab5e01c464ab3043387b6a5f3025294ba3169ba31fae28b2b96cab26a
SHA512	b60af63f683b3fc19837430d06a53168b0c63c34c8bda7fe5b46454605ff8d32246d7b62ccd89f716ec77553524d1f123dec3c916ceb2b81695be09e4287e62b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\21e378cbeed4f851_0

MD5	6161c48f0c451b5f3c3e6d582b2e41f4
SHA1	678ebb441aa27b66ed8b781374cdb79003fe7b60
SHA256	8402b025297b0373112faba41df612b178f6cf44f35187c0241bba08ffa6284a
SHA512	709ec84199442792b5c871504ccfd9242adacddc7e6464d3d3537d0bffd833861950436a3f8e809f0b29a1f14b3b392a46f82aff5ba56b9faa1adf5848c765e3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\cde1babb5a2b82cb_0

MD5	2adbdfaf66d19e755db799b87b3d8eaf
SHA1	46d4b6d552bf940a4bdcd95ea42d596019c7c197
SHA256	eb6c6a97825cf1c5e7166742319d2035a964c3df9bac4bd540c3318e3026f637
SHA512	0528e395af137a7f974d1ca1a7e82c2db0e75033c1f2d6ac908229f261d8f22e5b1adae256e009e05bfa4a1d7064081474865dda3ee1507689b4d1df0d761ecb

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\ba23d8ecda68de77_0

MD5	1bbae567c1012b1131108cf13a7be54f
SHA1	8208078f767ba6efab3002d48c8d2fb2bae9a8a4
SHA256	2b313d6964c6ca2255a4b48a9cb0a129daaa8626af1bcbb273332747c2fe5a79
SHA512	d120e7e493ff7931fc90029050ceb475e5939c3f0c9c4a8d1e3ec589fa51fd4a3944f3f356f4ad5f50176bcf516e42fda6f1cbd3210b2d13309f561ff228370a

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

MD5	cd07977bf1bc6722a9a6f80d2cc7fffe
SHA1	d31e10bee5966b4eea476481783e6d738ff2867f
SHA256	2e453e9740e07f0eed4fbe0501da89101f7af5a301695176ae80340ff8092ff4
SHA512	d8ee933743bb9b8b9e53c2db0ca35472598e6fd47ac4b8a9160da4b311fff0c5ee106fbc65d5634c465c977db6e339c49d1dc219ac6968e9270eb3151d2ca593

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

MD5	2090c102436e7290a4d23b2b0c342d83
SHA1	74cbbcecad46e39d925d6a529de3d9be83e04a95
SHA256	47737375d5fe62e7bd9172310a164adecaa202316e283412d08b6ccefa5daa44
SHA512	dbad38fc95987142a688c0ae3f61f2d7c799156cd56564bb93c035212486a36dfe8bb42ab3dc0c98ed310665c635593de3742c6089688d116ca5151b1fd37f24

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\72ebaee2-a424-47e1-be23-992ab157e361\index-dir\the-real-index

MD5	478f3c3d6e1370f744e14fb6b4de0176
SHA1	ffccfb2486b88a9cbcc2d7715085a91b1ab05bb1
SHA256	f0163725e103dcd7b7ac498d4d17de0b56b038472236ed96b1f328829a5fb308
SHA512	a5768b234f11ba4f24a926a73a85fe5c3490fd78039f5fd8ce7d735fc81ffbb49e6c91d38e7ce6c179f50f4c15374456727d8e14824dd8e23fc23383b72c4a63

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

MD5	f0f45e4a8dbae5524abd129321678448
SHA1	67de76dc05d3f390fc9a138afa83a56c307fae9f
SHA256	52c5a1ed63c75c20081e8cd30e9120a5102d182e711aeb97862b105a836419c7
SHA512	f710f7a1b164fbdd7dd23a615353116ae2c831c72c5e20c9262daa70b5d8544b58047f427a4797867ea71eeae072b71c53a9a831713cd0cc1986daa6a8e04852

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\a89f5693-9c51-470b-8ba2-fc7a0ccf1b6b\index-dir\the-real-index

MD5	92a0909cf0e19d2e8d2b96d41a54dde6
SHA1	bfcbee92083ea7f0383cb06ab48742e7072adca7
SHA256	45b6afc7795ce9b039951040cb0b42d0c8f911d4fb7c5839225dd697fb24d618
SHA512	1498c90562c9c49e3fe325d2935ba7659911bacf68ec08df12ff8beec42d09b08db4f86be2e08c2a529f920ae43f76a8899288addc2247c120b90e3e60c202b4

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\712e09c4-c281-49f8-950c-0c9b6737b27f\index-dir\the-real-index

MD5	b50ac42af87d3474d43347382f6451de
SHA1	e2b14702da5fc34b44fbcce080247f4f29f9f71b
SHA256	8c34047cb65ae4e4667fa6199c70427df45218c7fdb7fddfc8a15c9b4aa524d3
SHA512	17a09fd7ca886a9b0d665f0949c711b60baad87f7c7f28ea564635050df18fa7a2759e5337c75a06926941400e8ab16f5bbbe636065bf04ff49ccca54fddd93b

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

MD5	9bcc4cd581e57daf3eb092091a79368f
SHA1	a55c3eb542638a8693dfe98fa2c26bc81ecbed32
SHA256	b4d279d59b12c1725e1b58658a2dc14b5367b663e3093bf92895a1c3cf5ff59a
SHA512	22b4ded87b11923e129c02979a131cc0d48fd8aac3fc0384fa685a65947b6fa47e98fd27e180ecd74ee65dbe0a506d5d5a1d3e19481f5a07d75c7b6afe9a638b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Typosquatting\2026.2.12.1\manifest.json

MD5	d31707c275fda69278a549bda9d05691
SHA1	30fc20c9047508d0598e9b2a46e81e43d5282ed4
SHA256	c24447ffbc3d4a8748386c1e43f6879b4315c1a08a5ade4309548519b3da2533
SHA512	2a724812d769915cf9ef915644bff752f8b402c24f0b57b4c3018aa7e431ee03cc7aa513426ed29a653845ca8eb5e149ae78a51989e77b588aff641c2314c7b5

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Typosquatting\2026.2.12.1\typosquatting_list.pb

MD5	96cab41ecf6c1526898f2329f83bd438
SHA1	855859a4f2311d46838579fdffdd9d4f5dcd854f
SHA256	dce3a7edb33b0e1ee364cb683ff17df43d63e8ec3b3b23691bce5d312d2d2f3e
SHA512	67e6a480f00073ebe79b518908fbfdf8bb01d9c9ea110cda1b77cd0b94d3985ee6a07cd659ce4c5ef93e2ac89bcb986740e1d5facd142330ef55d82671ade5a0

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

MD5	67de830591cb0c00431e269f62237276
SHA1	c571178513b98544fa1115f82b7fec99a54d3189
SHA256	8c40d5380b35fb487c98b954381d4cea66b29f3463f7a4743c9acf84c8ce9d00
SHA512	d704ad9cc7d4f69767a72b6d43d0895781e859b76eb0306907af1ea157fb7976791ea6594cda146a32609a05b64f929bb62848508a2a77ba6d4dba7f029630b6

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\a89f5693-9c51-470b-8ba2-fc7a0ccf1b6b\index-dir\the-real-index

MD5	1d050aa65247fc5453d73a8f0e8a65ae
SHA1	531674abe239c8c82dac49ea0354ab2a1107d48c
SHA256	d997e10b4070d1012f78b4b6133622e40803b2f7b05e81701c7aa97e1ad91708
SHA512	17c228142f2d6d4a59387c62932f7f659414951867c065bfc6df3ff0bcff68217720375a1982ad67af48f87b42e611b0155829b9c09ee36719c344bf20acbfe1

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\f584c3de-1c7a-4830-b64f-0bb8a3f9b19a\index-dir\the-real-index

MD5	70da7bb3346d83fab3db99c5c1c3c579
SHA1	59797ab25930ce7b19560e7a4b69c4eadefad2bc
SHA256	381e7bd22f6e1fb47a1ba2f613652b6fadeb4abe49c7f7a92a6101bcc13c1bbd
SHA512	466cf7db9e5d5bca33c08bb4351b72309d3a16adb41c6dcb0637f6d8989c7f83240d0cb5910ccdf80c78444b57b5f5b726893d452ab56f79147276c670a98d38

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\a0a74304db73132d4bc12ef9404aa74f9fdeda56\23a8fe87-617f-4f46-a568-29dc9affefb2\index-dir\the-real-index

MD5	dc8072e5294aa72882a1772f556cb8dc
SHA1	d23c1343dcfa6d60af428783d1f7555d14c87fd4
SHA256	ef2ef32bdf3564efee73fc77997eaf4bc7eff3fd6882668ce3e4f48f78273b76
SHA512	53aba4fabf66dd41fc063ec128f8aec8e8a458781e7b4403eccfa7cd1feaf62014649266d3578766c81b03d56f8e8b9854cf757ef040569b2e4616fdca56f0d3

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

MD5	ba44ed69703108095520b083611943e7
SHA1	f7ad128a0a31cbee17a3eb3a1f97fd7984c051ce
SHA256	e84c97ebe5a03f2f72bb00f8ca818522ab4295e8fdc896e665e220b2276c2aaa
SHA512	041f00463d882a8db79f9cd2fc8f734e659410a1d02c286fc96826e57711a41331bfcf1df27b94df40022f862e20132a71e7c7703fed962bf528e14438c48aad

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_392829847\edge_checkout_page_validator.js

MD5	11d46bdcb9f1d19a351b2ff865b9b0f2
SHA1	2b498365ca6530fe83eb376740a2c0849e08bcb1
SHA256	24e61bd2cd840f1d0c31b656fda800ad032e71850768d77b04fc45c65ac1b3ce
SHA512	2a1acca19f93be135db3a81aa55c64e44f7f080f91d8d32ef8e8ec6eebc8e7dda7bcd064cb2e5ca16d5960b47bb4a204ff88e0ea71e8dca11cfa24dc6b06cd78

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_392829847\manifest.json

MD5	5f3528bbef6e8324bd313a94c0c4f4ed
SHA1	afbca5c2f2693b5a82e7c03d07213a6436981dcc
SHA256	fa91adfcc12fafa93d2574ce2ff6a08825701d997d63a0081500d219cd0bc488
SHA512	c2d020c7f46176e954d7ca81f493b711ca4353bbc2bdce1ec52dce6f2ea277669b3350444b8efc08a6d5a45ea664505cbe142353cf35149598499d1595f9c274

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

MD5	7bc439d3e562283e34235f8044777ede
SHA1	46a76ab874d0eea8b0b5008beb6c10529939f8df
SHA256	0a9bed533f734d2de22e1f3f8c819d4bb6d1cf16b0dfe4e7dafaef15f77bb7dc
SHA512	f44728cb842cc8b8b14d0169958ee97ac976cf429f7de69d531945146e9e7ad5459dd11f789e3f8a4456b7f98680284924e41d5185bf4a627a89dd8f0b4cc855

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

MD5	98ed0fc9e850fb9bb533ec2dcff6eef8
SHA1	863b729e8b73cada73df2c429e30be42207668d3
SHA256	f1f3be96396a08222238e2984c6fcf9c8d0049aa7c3d21501fc67810cfd690ec
SHA512	29bc981b31e1adc006a1daddafc8460ceba65938c9dcc8dbab155b85b327cce3f9aed4e3814a1afe041c44bb58c37d13cdbdb3d31b4b4a24e06746c1966b5e81

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_392588867\manifest.json

MD5	6658e8d6901ebdb2b695444e181b6348
SHA1	34c4bce8c106ad7c8ba03d56f702b868a9ae67ed
SHA256	a1774d7a0ac3f90fe6fbed83045377b838af48811380d5ad88809222168c22eb
SHA512	615aa2777141a88f0d0904e7c73de3affadab0e7bff76fd11b98c8970f9b44fff5186bd4ca721c8960f1b57b4e35323826d52d5fc09d10a25b21b4ab46167d70

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Subresource Filter\Unindexed Rules\10.34.0.81\LICENSE

MD5	aad9405766b20014ab3beb08b99536de
SHA1	486a379bdfeecdc99ed3f4617f35ae65babe9d47
SHA256	ed0f972d56566a96fb2f128a7b58091dfbf32dc365b975bc9318c9701677f44d
SHA512	bd9bf257306fdaff3f1e3e1fccb1f0d6a3181d436035124bd4953679d1af2cd5b4cc053b0e2ef17745ae44ae919cd8fd9663fbc0cd9ed36607e9b2472c206852

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Subresource Filter\Unindexed Rules\10.34.0.81\Filtering Rules

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

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

MD5	36d9a2bc426bc7ef4ec8babb10a7a390
SHA1	22451a8edcc1463e24a0520187e7d7192591be38
SHA256	a9f6c3941c77fa0e82f0251d0b0e5a68700775e8e062a920b094f04c1a121792
SHA512	880a6f0558e5a2da9db219c3abb963828f61642b730c45f3f623bdf732bbeb15a9d92809801fcee95520c16172cd3d95b2fae8c940b5efe620b3160a071bea1e

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\ba23d8ecda68de77_1

MD5	a0e868bb02264e5311171b05403b6566
SHA1	2fcabc5dcaa709c45ffb07c815f489b5ae59dee1
SHA256	b86ef3fa39bf97a21355b6fc05a5c483a27dc080f7d7dc1b77978597a765bda0
SHA512	d11c525d053020d024f8409ed9d95d30c4932577416835d336556c048ec5a44f73cd86ecbdbd00eb486bd2cf59cb9761a815d7d835d6fdd20c072a5665f60f50

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

MD5	f9c936cc12fc396d2005ee79089debfe
SHA1	184bf139c896606da04db31ec0d918023b4e7492
SHA256	7487fad5515b3501937d1e38512286b198721086e6585be0ef0f06939e08cb3b
SHA512	7268087fc2b7885eda7206a7124f973ed4f0c9648eec1a80d34846545586632d191524b279c2b57dc6fc4da08def927a36a311732bc19da090a1cfaeec5683f6

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\manifest.json

MD5	8083caaf7f5bc5f01ede464e68db1c7e
SHA1	ed6cf18f79c4ee2968adfffe7bf1bce163ef3873
SHA256	cd25cc1afcc03514d978f0a90692454e810c3cc81763074e0ea5ac504255335a
SHA512	60924bd5617ac5f994805f9a871999764ba93c6adda79c501a0b692dce51b9db6f6531a5e25129bc424ae7c4de868ba6e5a976d6bcfbac2bb8bd192c5513c7ee

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\Tokenized-Card\tokenized-card.bundle.js.LICENSE.txt

MD5	8595bdd96ab7d24cc60eb749ce1b8b82
SHA1	3b612cc3d05e372c5ac91124f3756bbf099b378d
SHA256	363f376ab7893c808866a830fafbcd96ae6be93ec7a85fabf52246273cf56831
SHA512	555c0c384b6fcfc2311b47c0b07f8e34243de528cf1891e74546b6f4cda338d75c2e2392827372dc39e668ed4c2fd1a02112d8136d2364f9cab9ee4fa1bd87f5

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\Notification\notification_fast.bundle.js.LICENSE.txt

MD5	7bf61e84e614585030a26b0b148f4d79
SHA1	c4ffbc5c6aa599e578d3f5524a59a99228eea400
SHA256	38ed54eb53300fdb6e997c39c9fc83a224a1fd9fa06a0b6d200aa12ea278c179
SHA512	ca5f2d3a4f200371927c265b9fb91b8bcd0fbad711559f796f77b695b9038638f763a040024ed185e67be3a7b58fab22a6f8114e73fdbd1cccdda6ef94ff88f3

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_580354290\json\i18n-tokenized-card\fr-CA\strings.json

MD5	cd247582beb274ca64f720aa588ffbc0
SHA1	4aaeef0905e67b490d4a9508ed5d4a406263ed9c
SHA256	c67b555372582b07df86a6ce3329a854e349ba9525d7be0672517bab0ac14db5
SHA512	bf8fa4bd7c84038fae9eddb483ae4a31d847d5d47b408b3ea84d46d564f15dfc2bae6256eac4a852dd1c4ad8e58bc542e3df30396be05f30ed07e489ebe52895

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Edge Wallet\128.18367.18366.1\json\wallet\wallet-stable.json

MD5	46ca0b1726448d9c7ed48735c246336f
SHA1	8e26f1f1c6f909f2f3d34c17e042e579f3b2b449
SHA256	c1611bb1872456d5ba656cacea801b833ea43126a6ad7e43e143d52cba9d9597
SHA512	c9ec0465c2c0eb0bc0316163f9a2dab9332c372dfc4ebedb0ef4139fe1195efdd8aa34367155c29e659d97d5a27e2395ce2f6012c115ef5791bad270de26bb28

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Edge Wallet\128.18367.18366.1\json\wallet\wallet-tokenization-config.json

MD5	ae3bd0f89f8a8cdeb1ea6eea1636cbdd
SHA1	1801bc211e260ba8f8099727ea820ecf636c684a
SHA256	0088d5ebd8360ad66bd7bcc80b9754939775d4118cb7605fc1f514c707f0e20d
SHA512	69aff97091813d9d400bb332426c36e6b133a4b571b521e8fb6ad1a2b8124a3c5da8f3a9c52b8840152cf7adbd2ac653102aa2210632aa64b129cf7704d5b4fa

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Edge Wallet\128.18367.18366.1\json\wallet\wallet-notification-config.json

MD5	4cdefd9eb040c2755db20aa8ea5ee8f7
SHA1	f649fcd1c12c26fb90906c4c2ec0a9127af275f4
SHA256	bb26ce6fe9416918e9f92fcc4a6fe8a641eceea54985356637991cf6d768f9fd
SHA512	7e23b91eab88c472eec664f7254c5513fc5de78e2e0151b0bcc86c3cd0bf2cb5d8bb0345d27afdd9f8fcb10be96feaa753f09e301fa92b8d76f4300600577209

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Edge Wallet\128.18367.18366.1\json\wallet\wallet-checkout-eligible-sites.json

MD5	ed22bc3ded6df0109b9e594867473559
SHA1	ee39eb80dc23f7fd764199cbe4a153c4edc2e768
SHA256	2abefae3d72e7c4f5cdc94eb0ee552612d843a26faf4a7bd061c73839e19d7eb
SHA512	fb337c0a0107dc37a3067bcd6f60ffb8f63ee892a0ff729dcdf67c7a21fec95a742a274853e8947489108d7543c13b9479e02574f490bc217e8a182f08543aa3

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

MD5	e903caf99b46792d7912268ee6f00d70
SHA1	b021cbc648391ad6d074d8274ce6b9c2fd78155e
SHA256	5c566be9ab5a3f16b28a2acd6198819278bb8cd699054f5dba459f730a5636ed
SHA512	5f5ea4b84aa3a1fe30e68628d32da06c2e501d4cb266784843cca4453ca7f5fca176f3d7e8d193d242635b7368f48f2371dc9d30b98f15058f3bcc943f2508c4

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

MD5	45b359a751b5af608fa32252f2d7d7cb
SHA1	60e90c0f72edc7444b391ff3e4a8affef4759968
SHA256	434b9edccf516de31f6b2ce93e43339d5fccae24f7b7c8c9505aa126e26534ec
SHA512	f811a5fbc9c22fb0b0b0d0d9bc9233ef81c9c159c5331b46fd70e43e7eebd08b4cce86f0caa372959e4b50323898ff647ff3273487b3ef29e49c0a824bc0b402

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping5772_1435100934\manifest.json

MD5	580786a5ec9eb650dde3e0e75db8588a
SHA1	8c0835d1a6bf82e753b624440e9674d649696ead
SHA256	25ac9b79df29fa869b4c9f4ca3bdbc3a85f6122f5a8efab5a1216d577099becc
SHA512	c8d41e16b291157e2afbf978469eae4c017d1ce3b941b93ae710e2bbaaf4c3e601db45e579d22b957b7a1ec48cba788015725a2fa23cf02f2d66010ef4fdd0a0

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

MD5	35c1bf65e2e5b741dfb790a5dc5c09dc
SHA1	f58aae24a34948e3d9b5ced48ea6ea8ae3776203
SHA256	3c604477f9f7857e461071da67ebab5ee297b820b66b9a060b72e895c4c6fd0b
SHA512	b1dcb0150e9a501b9427e8d20cd6929bd6fed0ecb71a95e821d49215de270eaef93802a3f32e17efd6c263990ddf503ae909e3218b63e0a49dc83f0d7f8b8d34

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

MD5	985a09b9eb2c40dd726f871189700dc1
SHA1	bf37d627245c63c87ec349a83f79b81eb2f4127f
SHA256	c3c306b71231b07899d5e2e49a04bd082f13b217c9999215094926964e559781
SHA512	9e7d6030d63baf8b6dd25e09c8e17c591bd9231dd110095b6797473925169d6dcf3e116dc471410858736f1a9e33aac2aa2cd3a7f3e9011b3bc5e880f715222d

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

MD5	32cae6258906ee1bc0b3c52de52b7c4e
SHA1	79a4687b144d06914539f1ed13a348f311d91772
SHA256	d92748890dd453460f7ed14c735b6ea02e26aa5f9ffe97e10053d32a7fd82265
SHA512	f6f9fb199a197245b86d3a672bb91d54fd1051ddcffdcb833e94a80f20f331c801b0e8deb27b626d8009be8d5cd74193f37e5942f142ad8edff36a12e3d03b38

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\d9dd2bd6-4a8f-42dc-ae4a-f28358bb8d24\index-dir\the-real-index

MD5	643b26381411a8095c024b74534bc445
SHA1	ed48a55d98f23231a3c93ee217f41a21c7fe9d99
SHA256	a6c84f06754851b901c688d3f34a89f519daf69abf0de298c5124e2104632efb
SHA512	bdc96e2f126c2bbf92ebe56a9999033143cfdf3a19267a533d4e6bdaa463c28b76c3b81b1246951dccc8e804e5dfa24cbcc8ef027368b10931ab54c281c4ab05

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\d9dd2bd6-4a8f-42dc-ae4a-f28358bb8d24\index-dir\the-real-index~RFe5ce74a.TMP

MD5	b19820f36f2a2085bc974a4a1ee22074
SHA1	ce24afb5da1987f2eb374cf560c96d9ff1867d7b
SHA256	d9185c8fc0bec851e2c37d57e0fc7b8f886000e63fe118418985b158eb07176c
SHA512	0e72134f7ddc4e1bf6b32042658b71c7e2d9204822dd441ea6c01e3055dce13cf136e9a57978512268ce80ef77e1f12044cc28eaca4cf5275ce2d10dc4049dfc

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Edge Wallet\128.18367.18366.1\wallet_donation_driver.js

MD5	03abcce3f9828372d9876aa2e6fcdbb0
SHA1	cf5834e1af5f7143e62a29ae0f7ede79178b3574
SHA256	39a63d56be4f1ca950310f385e8a42f7bc2dcc0e49fefff306176182bfa4f0e5
SHA512	ef9b7decb4cfee3961006ea5c77299a48fe6a667475772f2a78e93bd4f691dc4700f8008138c574898fdcd8d717d84b8b201527ddb5a61346e05d362aeb15701

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Subresource Filter\Indexed Rules\37\10.34.0.81\Ruleset Data

MD5	135db4e8520e0c6ad4abab7bba2c621c
SHA1	ac85f5b7858165aaa8cfbdde0919364ec14654c8
SHA256	54bd9731392c3850fc347fcb09c4dd558c915e742dc491ae4173ba1f00abaa50
SHA512	2bcd8fe87a02350c49a18327b614294530721c9456487732108eb0f2c4842faf2b329f04983f36f46424febcd59c0e5e14d69a9f52e60a6dfd161926ec6b7ce7

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00008e

MD5	34a3223212688ad49ef71ca1cfdd22d8
SHA1	ec618405fbfc575962d0a394170b11da61d80544
SHA256	21724bd3c48f76d7a44977aec4b69d0d7855c789e89136117d8ebf052d547364
SHA512	3188147bfdf2d748e5c3d499bacf65d8eb128a5fcf3fa3c9bed9deb7695e542e282c247a29e99b9fef5d91f1a46b3c9c60718cffc7c5357aa7f7281e59031e54

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000087

MD5	502e615e085f1ee9e7639aa7c750ec03
SHA1	0ed78c740179ab0a6af0db8c26a7a7f271f0571a
SHA256	7fd2cd52bc8a1a14c0c921c39667172912ad7d5a3d1e4b54be9ea5ac22c3d84f
SHA512	91c9a98252466386fb05b1952b5b4a93006615c34e63d9ad08449477c92406d46999afeed9a26a8c5106592b5886baebc12318fb9e3d753d697217a4924135e9

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

MD5	41ad838a23815fff83a6b822aec9baff
SHA1	18ba5f7010111ca82193db4ae151b57d9743efb0
SHA256	b7303731a57e75085beeb11bb76d7c59f3010e44dca60461e8ef6b82743558d2
SHA512	0e34a1252ea3761cad97127faaba7e652da8f86d5463f05a2030f5c94d25d0867cd8a55ede58934d4cc32dda55a785e4f30670221f58846e4d79ab9fd496b1c0

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\RevisitationBloomfilter~RFe5d010c.TMP

MD5	55332dc52f24901f0c15632bdb34ef58
SHA1	2d670593bc95fe65d351e159c99a90bcbe6eba91
SHA256	861347a293f05a572474f45adc6fdcc901d69a4fac75577a4adcd290e4904fa3
SHA512	95b0c8e173e9094f91bf3407b737da8429281a9c079c7dcd9ed2775013371b6cbd05cb1387276545df2b10d198407ab954bd641349db58f14b777a3e6303eeeb

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

MD5	b66b88c2beebcf2f59d9d3ff95a10e49
SHA1	49972a269ed59c2449595d0dba5850c18420fd7c
SHA256	f04f278715255329cb73e66b1c1d8cae2bbc81085cd01ab485c7b1d519586e3c
SHA512	b42508623eac321184343a9fc36614f77a97c93e64393b750b8732720ab41cf11a6a7dd5e5f0ce0983e5962466dc2b1c206e8eefa8f24294d1d80f04e2d05c0e

memory/5424-3396-0x00007FFBD24B0000-0x00007FFBD24C0000-memory.dmp

memory/5424-3397-0x00007FFBD24B0000-0x00007FFBD24C0000-memory.dmp

memory/5424-3399-0x00007FFBD24B0000-0x00007FFBD24C0000-memory.dmp

memory/5424-3398-0x00007FFBD24B0000-0x00007FFBD24C0000-memory.dmp

memory/5424-3395-0x00007FFBD24B0000-0x00007FFBD24C0000-memory.dmp

memory/5424-3400-0x00007FFBD0180000-0x00007FFBD0190000-memory.dmp

memory/5424-3401-0x00007FFBD0180000-0x00007FFBD0190000-memory.dmp

C:\Users\Admin\AppData\Roaming\Microsoft\Office\Recent\index.dat

MD5	96daa8d2bfbd5586224484c05d19f09d
SHA1	7b8976f6eef2f7eda949522b410ab4c50b102315
SHA256	3b089eb14db96cffb11e33b003433138c01fd382fd3ed2a1525feca20ef31141
SHA512	5aa2cb397989a9805ec375f41ac5f1c3c0d2fbe32a577a2448b4ec8b9988ba42b3c7a6e5e06060fd3127141e7e65b355259d59b50893ba13cb44c4cfe0ae7b77

memory/5424-3439-0x00007FFBD24B0000-0x00007FFBD24C0000-memory.dmp

memory/5424-3440-0x00007FFBD24B0000-0x00007FFBD24C0000-memory.dmp

memory/5424-3442-0x00007FFBD24B0000-0x00007FFBD24C0000-memory.dmp

memory/5424-3441-0x00007FFBD24B0000-0x00007FFBD24C0000-memory.dmp

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries

MD5	27a22a0a3ebdd188c63b36c33f8cea21
SHA1	e8eeeb0c0d90d72802c25f74507ddbc6e83e6811
SHA256	e242039a1f75d12cda04d87730fc2d3065441260b2144afdd726e13eec008810
SHA512	cdd302162873f0e1679670e38b8ee38b1e9845acecf01e4e649b658d109afc80995910f925f8eb16d66ff2110e13360b818e69ac362eeea9f0b033d221afb761

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

MD5	9020623972367b08dc748241ea8b7422
SHA1	5a784652eac26fb22f7b252c160ad701ba6e03fd
SHA256	69ef247f88c7b92adf0220bf60411e603a9b8b18083eef41bdac3f5a38bdbd9c
SHA512	babe049472af0ead6aa716c35068ed9bd63020ec82e7c0cb0d51d4ad29f39948b4be13d929b95476bd548c2b2af249ca33b6b774711617d9c7ae3bf679f6259b

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

MD5	7bfe0c1f2114d67c8d2d904c9f635b6a
SHA1	d024355fc370861558fcfebdb5aeabd0eba4e32d
SHA256	81d5400a673878ae56b1e9e34f1578ea54dc4e0cd32771de2fc6ef1599ee4753
SHA512	9df28d4ec104a46451a742462568c7647fc87069605999ff1326f2d07e5bee3c704f42696a898203442e86562d5573c8a52d39af43389db5dde0c8e103360d1b

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

MD5	3d463ec190c05e304013ffae5c9fa64b
SHA1	e306473055d0c7855f2a6863907359fd00a48c3a
SHA256	4bbf538ac77e0b1ac6265d73c1f1427d322f35057e4ff19421927f405b3e2d25
SHA512	593ad10e3fab39a66dacb8e9a9d2f315cfb061335f3d8dd223520df37e8ca8a176ce28cb03f731c9f85ed1404d3d4a5ca236fdd26d17aa682c01421aca326d59

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\d9dd2bd6-4a8f-42dc-ae4a-f28358bb8d24\index-dir\the-real-index

MD5	3271e1d2c2acf1f0a2f2c7078ddc3693
SHA1	893627454161160f051d3bd91e34d2f5a446d06c
SHA256	7aac4ad2b9e67aef83b281509a8712b5640935f6236a40cb75764c38d25ef785
SHA512	4e1454c3954997fed218de8fc677f0f8a01ffa6402558100fd4f36508fe71e8416bd22783b93f32ec942512df594cdf9c656220edd347765bd2fd0ace5249c1c

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

MD5	df9beff032e43d21abfe2a815035845e
SHA1	ed2c93f0b57d2fc4ffc65e2d5cfd3731198bed00
SHA256	5c6740bfe7541ce8d0e872af37e912632c1896df7f30fb7420ed0b953d45cd8b
SHA512	d47bd7808dc0b123292185bd7f9acbe442b25aee2b93783a51101a654ad0ccdf8be690c969f21b6bfeb37982d1398e68d640b53bde90a82c766ec2f62043c7ee

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000099

MD5	b33541f653e14435c2adf810d572107f
SHA1	badaa72ea319d86feec193726bf9b87449349bf0
SHA256	9cc228031f458fd83b91807a8a75e0e010e8c7594f53778ecbcd147da1394389
SHA512	bb4a6402d2b3c720197469a571ade4720ce0b4671462f25198f67f589daa4a7c49840ca9fcee970b2a72967f75c6b347232983f147a7d140daa080026943eb96

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00009d

MD5	1bd4ae71ef8e69ad4b5ffd8dc7d2dcb5
SHA1	6dd8803e59949c985d6a9df2f26c833041a5178c
SHA256	af18b3681e8e2a1e8dc34c2aa60530dc8d8a9258c4d562cbe20c898d5de98725
SHA512	b3ff083b669aca75549396250e05344ba2f1c021468589f2bd6f1b977b7f11df00f958bbbd22f07708b5d30d0260f39d8de57e75382b3ab8e78a2c41ef428863

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00009c

MD5	226541550a51911c375216f718493f65
SHA1	f6e608468401f9384cabdef45ca19e2afacc84bd
SHA256	caecff4179910ce0ff470f9fa9eb4349e8fb717fa1432cf19987450a4e1ef4a5
SHA512	2947b309f15e0e321beb9506861883fde8391c6f6140178c7e6ee7750d6418266360c335477cae0b067a6a6d86935ec5f7acdfdacc9edffa8b04ec71be210516

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00009a

MD5	c813a1b87f1651d642cdcad5fca7a7d8
SHA1	0e6628997674a7dfbeb321b59a6e829d0c2f4478
SHA256	df670e09f278fea1d0684afdcd0392a83d7041585ba5996f7b527974d7d98ec3
SHA512	af0d024ba1faafbd6f950c67977ed126827180a47cea9758ee51a95d13436f753eb5a7aa12a9090048a70328f6e779634c612aebde89b06740ffd770751e1c5b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00009b

MD5	2aea4a78f91d03584bc1a0cd9fde58a9
SHA1	206194965552b7710c2bbae795e522b3ae667df7
SHA256	b3f1f7fb3d9194255bdfa9024c88db7558b3102dd35b95a7e6a46cae5c476b19
SHA512	cb6b68748cb9d0b518f4c9801cb253bd38900b7a1b7907b8f8efb7150077d74c0e6e5869907ed1742e7827ad9c815575b5e80ae642a2a46cf07f1d9f11711846

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000083

MD5	e930cf00b9f1df58faff97bd4c06db59
SHA1	efd2155e9faadafe1558e1c5e5240e4f01db36f0
SHA256	a41c0edb4cecad4f7644eb7348e57331065814d38c5716962098990b320f4f0b
SHA512	d402f6493c039f2c59381ec6ded80acb410cb95834699b5900cfe305fc1cc9d59e4546d481d46c11f1e4eb7e5f10abf923790998eb2024cf22a3e3b4f5551308

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000084

MD5	2f2d9b150f028a497b5142348114143e
SHA1	04a92f6d8233dfe2e3b40a0d9e203f4fbefaf63a
SHA256	86ddc4ef4d5f4505ccd6d98ef2ea09d761ca9e2f950c2d287693e69b8075b930
SHA512	a6b04959ca6a881e471ac8276007b5929d669becedd547524b6e0a371902313c928c757ceaf39cb428ba86ee5d03aeacee98770938307d87e35ae3e449ff97f6

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00008b

MD5	8c41051a1bbd9fff6799fd85d36f8648
SHA1	2fa5a5c4ba4b03315a9224e8290dee12d9f05f66
SHA256	94d940f4272a9e22b36020b4dde665200ca5534ac2ee0488950cab870d32294c
SHA512	5edc51d37d4ae9bfebd56a3d0bfb764489f6e9d2f333e79e6b420bd31050c303b65d2b434863784f0e40809819b81e47e6399f2827e37b883790c3a60c5dc638

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00008a

MD5	d2bbb54320e3de5a0f67f6bd85e26a4f
SHA1	d4c39a648f05d224539236da088b60aa03360d12
SHA256	b912b5bcbac3c3091129b3a6c991eea88541d53d0aaf63ff3102957fa5d04429
SHA512	3347c3483010f5c58a7f89ebb0fb7be75ee5bbc0380a1c4fab7bf1e94719706fd71364fecbea1626a034934f81fd0eb8c1a76baa3bc2f4efefa49f75c297f478

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00008c

MD5	bd69312286b55dc6ca731a9dc667a5bb
SHA1	2b1f1d11bb3c23762510c5dc74157f0ff59ef42d
SHA256	3db4f424407ed222db526ca84d9419f95e52be451eac3b8ab3837899dfd34312
SHA512	d76f71bf1f63ec45027f5474ce3b56c219bd8e0e5566d47615730a83d4cf5d39b780765e31dc9f3f0845b48131b27989b9e3740225ea5820055522a22265c42a

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

MD5	cd021641b4742a5a543d2630972b75b4
SHA1	e8bebe655bc8ce356c9c70304bfeffbb065067e9
SHA256	d92e9813f6429d9d04eadb6bd06c56aaa85cc998ca5c788c71de1aadc64999e4
SHA512	5ea397e141ab35f13da820e224a45a5277ff4b1bc7133a50dbd98ed11bb5e0afa3433505459ca3314bc5d9d0b784fd85127cf59fe1572db5a5b18894d637ef88

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000090

MD5	c21d5d29eb3014fdb864f388b34145ad
SHA1	85f724b019e8d04f50b336631c66f788c2b8f651
SHA256	542ac655cca6f4835f0752937b8144fa3620dfec1b42b5277470217010a621c0
SHA512	a67da76326688dcd2de7ab513669246bdaddfda93635de9ef7db820243f3c4087e6166836f8b9cd09830873f0b375d2b720241734eb50d5cc8340d0592e9dd3b

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00008d

MD5	8ad90e1f14080c8c1e1bae7f97f962ac
SHA1	9f352466e3ae876156d238386ba7d07b1574e30f
SHA256	69c3df0acfa9b94fad710cd600e6d092b54a3848415a3c7b9d178cf9600c58bf
SHA512	f60678296fd28e3aa7e77177867a3171df47f454a569a0a0b3d8ca5fc2ea6312a6ae8ab4f18d887bb5e693aa27532a94f42d6912aafea324ebac35895a68b529

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000091

MD5	be569398e0e595dd2f72e1bc4cb2e4c7
SHA1	a7a59eddb0ea2dacb98ff03113480327c1805c9c
SHA256	f3fdb11faee00508cfab853c284debb72a6054ce7a437005f271fdaa419c8c9a
SHA512	475d255ae27e373971a32efb3c28faaa9aba5e3b6790329c211e038d1258f84b826b88aed8c7451749a608dad9aa433b9454520314c20339fe6527872bb15f61

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

MD5	278c77913b10924e27f7b5f6e0bd24a6
SHA1	bd0aea3876763308a079458e993dea598433f113
SHA256	2231928a19c8f40932abadcb421fb4295d2fe833ab5a9d311d07cad92d4fa0cc
SHA512	0205d7311358ba07b5ec19e901e281ae32606e79022b472379f8802799c2e9ea68a673f185d91df3c9b2fdc8db7e0df177e6a3f3ba3b32255a0de57aca2e9bbb

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

MD5	0d299470e0a7490f0e64d8a184900e58
SHA1	8f734d108e2e6de6a1142623ffaec59b31f80673
SHA256	b14b76a814f3889e3dc6202e1ef011ec226470766a7fdbc0abe510287040d20a
SHA512	bd9e0a8933d2a686f31603ac15c07ca720c371f24876d1725e43cacbd3a825c09ac6f55e0f0aa89d7c578345cce88e958c1ba3b9b376a7637c5af5458af64558

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

MD5	3f472f238df4bc6de4ac42251a18cfe1
SHA1	2b1afacf69adeec26154b879e5fa4b4e40f36d1e
SHA256	63f645c314ef19ad93d2646fd7d8db17e69a95761f7e48d80aa49a745738a5f5
SHA512	3de4346b4efea4f249467689683e9665d4fe24dd228ca52dcf22665319eae4ea6147113fda4527959184a8b2ae2d99cdec5cf51334924a9d143c79ecd8da5879

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\42bc61a2-5cd1-4bcd-8a9f-064e87b4a21b\index-dir\the-real-index

MD5	96fe3f7f1f55409c3378a63c92f0e375
SHA1	74551fabeedda4f0438b1626322d36e975153f89
SHA256	2cb64d3ba9de8bd1c9aba514c0e04a3c982313bb08264c9d72ddec225c130868
SHA512	8637f717ec6f90ac4e530215cb5ddf5ed2bfe58ff1d0e375cb08d40af7abbb7179c45ae4d65acbfc8f1190b9400a807586fe8aad949d947d48a7ac556efa81c8

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

MD5	225a3d4786a29706265b8d0de24e5ef3
SHA1	b176b45bb2ee6196cfbabc208a1624e403e2c0d9
SHA256	35218b96ce81f327c1451956850eb6bbacf17214b36e27fad1d63d0b7329c99c
SHA512	11f96a2182196d3c4c6489e41b13396722c8681b8d687a83c780631316f04e6c82e013dc7f8fba867b57ab64c493b58048745d655c686e34953a9f19dbc7476d

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\f9c38cd1-a83b-4f7f-92a4-0c47db01aac4\index-dir\the-real-index

MD5	ab4cb780e812423e7c3df9bcbab25255
SHA1	bc507933b9d98e2baa8ed6b9099455cb580e039e
SHA256	d94225c1fca88d00b0094f7ef569be8914d74a0d02c9a603a0aed07375417aa3
SHA512	1a4cbe832f76edb6456db0d57202151cc4dfc2223fa2b17de4103f58b2994dfbcda25d7f9d4c2426b9e37331da1712bb5a47041b21170791f94314b6a89ae811

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\f9c38cd1-a83b-4f7f-92a4-0c47db01aac4\index-dir\the-real-index~RFe5d714b.TMP

MD5	8298ddf69304b7b0491a520f6c6e20a7
SHA1	e167ba297f0be41a7a4839f97fd1adfc3413acdd
SHA256	d38f18ed461a4a01455c37be0e2eaca4acbfa13ceeed44c593764b3f18c53c48
SHA512	d6c83ba24c74abba2d26d1143dd97fce34648a5d0845b7e77b82080aec231cf130b09055a48359a7367a1a8d21ebaa198ee10b5005720e570a7a30f88f8aa505

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\6033ab9d-c3f1-4d79-8fd1-9303c605965e.tmp

MD5	68bfbc1d3bd47f40fe9a1bf9835fb31b
SHA1	924edec1d2fb5a96279f33f5ff9a3804327190ee
SHA256	dd082d3391982d639001ff1c025dc26e08e6af95d1b5c493853a3ffd549c0504
SHA512	53bf73ba60ebcb764cfd928ffc3c063c4385644211a7cfd0e4ddc833b17c47bba40f1c9edc15216d186fab37e5ebebcfcce4e597c1d4517bb0ace3a2d619613c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\42bc61a2-5cd1-4bcd-8a9f-064e87b4a21b\index-dir\the-real-index

MD5	6a3f0d1f4ad1dc937b92ee60a7e34e43
SHA1	90b140846fd4950233c9b3d08040ec3fe8e7187d
SHA256	375a371c8ec9b12c1f5806ea10cf4244dce47f25cf0dc477e759b1f2d25d8f19
SHA512	eafd2d881d8027bb5d17fb9cd6e74e8b0c0e7cfa749cd372aa7af05b802dcaffacc0c84460bd9a2dcf4441da1d985be2fbac1eca97583cd515d57782b64def5c

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\3dc58f64-1ff2-4e93-a39c-0d0b2a8f2df5\index-dir\the-real-index

MD5	15ce2729eff197d5e137e4cd81f3f6d4
SHA1	f55a3fdfd959f1f3e7f3e3d89669cf721edfe108
SHA256	56d16ae7658e0fc4d81d5d85bca47061afc2aff2dbf41da0595bca5e46d22a47
SHA512	c131b4fc1e12a429dff1422408488b9e8a32b01e6bae6f7d261a32b90b06b3c35363946e0af42f63d2d7d07684f368f842b9efd08a38be953ac7e7e47eabfbe2

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

MD5	16fa29cb837502b64a18e790bf1ec97f
SHA1	6e8efa2148e8bd9ba82c681a2a3596fb12438e4a
SHA256	d447010a97b1f73be441879fc8e45c137a19f9de45c11aab82fb9ac787ed9aa9
SHA512	9fe431fe5e0acfeea7b80cfa12e65f117a688fa257f535c86dc44c13b8c7f19ddb244d26348c5e487e4714c70ec2fa19cec5102c4a583fd4d14c34216e311045

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

MD5	1a507adcabb125644a64acadafedf67f
SHA1	7e1470176fd0683c35137bc3b5231eee83e4b3c6
SHA256	cc0713db4c8e79ad1e4f658fc3afcec57d6a7464cbf02771a7dcc1bdad883b7f
SHA512	cefdf46b1e3e0049248492ae5b078692b1e1b5ac27c58410b089b3da278311160881740fb72d6d9f9cc3e45a72d3a5b20ac24230727e812baffa46a748774d3d

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\ShaderCache\data_1

MD5	27adaef141abf507197c1b7f776ffeea
SHA1	1ab216fb0213697fbaa3c6a3d134fdd861598947
SHA256	f261b5cf1a8aad4c62cd2e0660201d65e043225b4b44dea997f9c70a8c0e2e5e
SHA512	10bc5cefdbeba62c9ae241d93b5e0f47e42f3bf5f6ae48e51a7c0f21addb8c80260094d01dce81a5e82aa3cd8969d8ab32fe42c521866aa2e8b46530a50a664a

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

MD5	133bcd3e747bbd11b9d0c2c80f14b561
SHA1	3cc061d2cd6ce367781275c13bd57ce07f40f617
SHA256	a63e4723af7d2d4601d88d8d74932d103b5d98b9da021df12fc08e138718353f
SHA512	b8c4eb90757d8389b531f44bd2d0033f9b530033a50ba89b87a44794c97f6cc1ddd3a929ce4a14fd3fa85379c0a43b3ea5ae85799ef62bad76be266bdab4ff33

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

MD5	961e3604f228b0d10541ebf921500c86
SHA1	6e00570d9f78d9cfebe67d4da5efe546543949a7
SHA256	f7b24f2eb3d5eb0550527490395d2f61c3d2fe74bb9cb345197dad81b58b5fed
SHA512	535f930afd2ef50282715c7e48859cc2d7b354ff4e6c156b94d5a2815f589b33189ffedfcaf4456525283e993087f9f560d84cfcf497d189ab8101510a09c472

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

MD5	280b8719e5500e3a1c4b2fbe641c8580
SHA1	d93e847ea9cca2a3c4cbe1c646fecebbf8f30c31
SHA256	798fd85e9d437ff7dff8f18671cf638e365fb0aeb193e16ff573cba432cbbeb5
SHA512	caef1df80aa376d04b7609ca996b281799f6958215d536ec7f13768ef851a28b45b1128a843d3e6c3a7bfcbe831be74b0b3c13c03a7f283b4b93bf2a80e7e4c3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG

MD5	9e335351e07c973392ef2e9b55950f0e
SHA1	280dc05cd42887c0fc1518dbd4169d92d821043f
SHA256	14faa4c3168d8db35db8ef5c281b4a79798a96563c911b1bf79b921ffed07ecf
SHA512	d72e88eb962e4fdca685762a7aaa2de495ece92172e9ccc569c93b535766082d5463e597765e1a670250abcdd7108b953d03125943502e505c907c088bb47c53

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Nurturing\campaign_history

MD5	5ea47d237e34ea52ab71c531f6329766
SHA1	33adb12087594219ad75eeb3ad9188b822d1e6cf
SHA256	b98a97e562361baa8b6257d858eb5f05a0451443b265b3295e7a12970a7d9ae6
SHA512	6e4af3ebd29db4e2a48e9a99970b0a9136b28fb64733fbec5097888a8e81f4cb424fa1e67dd3aece86114bb65b2ac7a568782962b27d16af16ad1084b060e7aa

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\000003.log

MD5	897f54724f662f660c30ed41114206b7
SHA1	dabaf0fcb780cbd4c56a26b9e1febc53fe146849
SHA256	9b85f88fc8939d8f4e5dc2501923acb53bdd44bdeed17ada3db234e17b0af8b6
SHA512	11943cdff020fad7603a625ce5c4d0701019de6189ca71e02db1703ba1e5e9ae4b2144afad8e29177f2da8c3fea29419f535843275d9cea727a7440d3ef980f3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG

MD5	b53eab37b012ca8e171c78ba4aa829c7
SHA1	6ca6fba8dd1f52afc570c5725b5ccc0a54ba72b6
SHA256	96dd61138066b5a5294e080923183d2489f023f0c64ac4c630540dc9ebd97262
SHA512	6940197bc90430dbba2b3ff6619136573066cceb873cbfd52725fbc27f88f6290275f89d7fdbf823934075994c4e6853af2546701614389 07f03e98a6d56244d

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\000003.log

MD5	16caf873f5fb226370277953433f86b0
SHA1	0b871fbd6f127f33e52740621ae17286a87f7dfc
SHA256	d63e131025959b20b7fb617f4531db04d589e3ebc7ae59a6e7f30d11c92b7129
SHA512	17400b1c29027a20d933192a9645f313408c6b969520f3e0ee4f8796247405d4fcbc63f7ff7e5b90e65a103c868a0f8f52ce16cfd4255598f546a783f86446b3

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG

MD5	84f08b1ecd6899a7c05d4d6a4917bdc3
SHA1	02f93fe8e31a502d398fec9ae4a19a485f71945d
SHA256	ecd26d95f4e76f0371365c01fbc40e9ca431717b0ef4ae94558d93b6df73c2d4
SHA512	605887df1dd63138b1d31b7519ed3ccfae49b8dea73a43408c78f910992b7dfd55baa263f890c2f300e9f2dfa897f8b5beb4212d81920709f4368398e924e85c

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

MD5	6eb7fdeba5743dee07c3f676eb338a27
SHA1	5277858a7d3e121a2ee760ebd4547bfa7b862bbd
SHA256	d317e15adc4657b10fe8cca37df3e0c6e078bdadf85662d0cfd3f5b61f3aa08b
SHA512	50b6831da6c2c8849368cb93d7e86b576c40a11a9fc319b11729813cb096dd94c73ea15f8d95b7431b1ff2ff383b44c91f50cff6bbf4b5773f68d04511065507

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

MD5	537e0c7892a857062b578ab76ef191b0
SHA1	db037b7324106451e4d6db5e995e14d7e486ab90
SHA256	58f34b339f2912d794ada0ab2659cda804a6aaf7a9bcd67ba32234f105f8cd6a
SHA512	183fe729261650b8ee50ec6f94c76186e6aef2e5962cfc922183415b701f51eadee3610b9c46d49878aedd2a538a34c2e8e445d3110e276f14d4c2136665f7ab

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

MD5	2b662e5595d8db7a809ec98e66967c08
SHA1	df4290206e1f67b1e35ebb767650c704ea3d5ef6
SHA256	01ca2dd6f7d6f62d05dc30ea385292526e8ce44beaba9357deefcd928f717aa4
SHA512	4928583e4f8b5d0ab09aed6037b1bd8251ab42490876c50aa82dede79c62362e2d21a5758473e320d1d93d357b4c24a322f17d080c648be238bb8538a5ec22cf

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Last Version

MD5	8297da058a737611abcc3a0ede9ffc24
SHA1	e532552672ecffbe3509fb4c334833a67f16d05b
SHA256	ee1367d356a136a11664001cd90e05ba08dbaa85f496584158f5e42be8e836fd
SHA512	fefc70ebe486693310a00beb5ae125abb1569c4455538124d897566f2e44f2b3854ad4451196607137301a811ac7f96f1d488a36eb6d6cd566f2f7cdc7c7568f

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

MD5	d2a06293e5600ff2effc2330f7f2eb32
SHA1	220c00c97f7cf549320b94a64080e376d782b0da
SHA256	766a4df7274589ff22a563ddca606db28327949617dc7090916e3b0a426d28d4
SHA512	e92d326c5213d591df380335bfdb7f5a825c00f1a0514e367a248bc2f86a5914ce635ea6d04231fd3ec86f420fc6c90e41dbaa957812891924f87bfcf1e1aa75

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	66d8a34123b432dd1d0e9c9f712b7c64
SHA1	38941767b5ccc9d2bda42864e1899d5cc90f7bd2
SHA256	194d2bca07671dceac91c8a21f9e13fbf75d01391e61165eec39f2f64a9bddba
SHA512	28427da7743f471ab48d034a023c2daa1a75b917eb016155891ee3fd32172493d251732b4089a24b6d47d3ba5a49e06fdf71922a0790b51d552102535dbaa4d1

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\BrowsingTopicsState

MD5	dc97c1032a950e67ebaffd836ab6be76
SHA1	d655a2c27a77cfa48d3076c510a94d4695d314c2
SHA256	8a7a9a8aca1990096a759e23a439a3339a950e94fd6c6094da5210cf6bbff27e
SHA512	a7dac59a148218269ffe69a2e29a459b2c7d2003c16e49cb80305016a89637206aabfc2901549a0335fb99d28aa21f3a447edaa3c91736bdb77aa63a1abf12d0

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000008

MD5	9705fae224be8bfc9de7353dba23d1e7
SHA1	d9fd6c186bb8fbf182041bd250e674dfcab53766
SHA256	c6ed9ae80e488e07b3b4896120ce4420e137010975c296c8f909d67430c3a1ff
SHA512	435f47765700f02e892fdcfb9821491026fc71b7e0c47b83c1995d8dd9731a7c027d4a792ba58efe1c4eb0c6852ad756fbe54c39b701bca87886a839ebe6595f

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	fcc458959c256ce1e4ddb4311723b4b6
SHA1	2dad47659f5dcaa9e2628c004b21c35b1ee6543c
SHA256	6d53513270c88dd8739f8b124b45cb7629a1193636da7506cad80c07c0206734
SHA512	e659412dcb03b3bdf4731d9edf3df6e6f0274f5138b323fe65b137e03da07513973887ee79124115f17e5e69fd66c316dcd6ddeb1a58f6710a0aa3a7ddbd13a9

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences

MD5	b0d1f07abc4aceeca25ae213a8bbac55
SHA1	a12bc0ba5cc6482694c623f530bb61f84aa919e1
SHA256	b348ef89a2004de3932b2d422cfbadcb8511ef1f7a57517647d45e46cced5182
SHA512	31718e2157284309c07a2a635a298c85d9a7fbefa24d929b57b0b42e496770d473b3856a02414740260339a70352d551dfa116ce6cda0e72e227cf4c48e62db6

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	980b3cf93c9a29f8b5904430f3533994
SHA1	20ccf3a1133c8ab5dd3768f57dbbbb235d62f731
SHA256	e2575cb77c50bc1434eb7baa8979bdcb42ca932cf739a9d82c33ed2f9e08d794
SHA512	9744ce26353c6f7e4fa5c3084664962ec1b5dbaaeb94364d3d4204ba9b0d907db2a773757a9d7286b29f4d936a3824d4f1860766a52a0b29126481696fec9b08

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

MD5	7c9736895a25153743e525614bc4226d
SHA1	2fa3e2b730080752d350bd2aa659cacbcceee5f1
SHA256	3c9c46d33c31ecf3f09da27ffd4c6293e2731f4da6f964394708b4d72f1ab16a
SHA512	72a60d5f07d610ccbcaba0aebb049c0b8ff7b939ced743e4f3bd33c7c755babe3dea9a40a94bdef4d317448dcd99daaffa270cbcaedadf510db7c45337f3e993

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index~RFe5dda94.TMP

MD5	4fd7e1ca1b7bdcbe8be3ab5ff53b91b6
SHA1	d5a3a3e721c6f4ff1b88e90a668c6b183f2c7e87
SHA256	a4413fe114b5138d2875d7429849bc6a2d193fcaa62303d8bba497c4968f52fb
SHA512	843960ee9a599e8d0d7b6a96531a4a5d66f63f317c1e449f57d080fa835401db56b7054238e84fa109319dcc9ccf18539f4b5bdb548808af25b42a7fc40eee55

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	78e9abba6d4266e7f55035c1e29e811e
SHA1	b6cc194b4e758220cae97c8c67f6802fd760ea55
SHA256	d631b699b6749ee8e9d06e5caf3ddd9d746655da3b2eae3a70d67d03b844e2c4
SHA512	ae56c15cefa5d35a26f543c0a9aca815dba2ef9f70b8ea6bbd64d6e17ac680a0dd87ddb632eb502e944328ed7a76d255421caeedfe7d821312f990111c864fef

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	0186515e15c007148e5a1de2c1d31b60
SHA1	482b68576ff863e0aac563c26ee97a6c95f5156e
SHA256	87ad60cbb173ac973c76834271a57bd7ad9c72b0f4d170d3c1569b86cdd5a0ba
SHA512	4a55b7bd0caa819c614e6547ab526ad834ce110f38245cae0255ce9dfd487af1f2cc456a3663b28c943c2443808c4a17c4d5f1fc0784bad285f8e31655bbec14

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Shared Dictionary\cache\index-dir\the-real-index

MD5	41d968899e9b7e913e33cda041ae1c62
SHA1	d6174a4d76a03d0d6e39f742581926f248d0876f
SHA256	b7cd128540f4314b86a9c86ece007b035660e177c0bf2bd7d049bc788caa3054
SHA512	93360206508cef21b77141e768ff089e429fcaa1f70e37c21388020fd6810cdca0a02f10c2d322bea1101f2cfbc0cd16020fab291b4cf276dcb666349c87fbdf

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	f79d671aaa87f81b221e49d28f83edc7
SHA1	72af6ad1ea08fb15129cfc53cad291425582d5a8
SHA256	3815f76055cce7b7e4452996533203c3df4e929ad33eb14362568f9e5eb93106
SHA512	5b373de4b0d6386440e8d84e41a851e16df23fad9bdc86edb3cecd62b87f51fb9797d051f38f3fda19060b982769893504377f5fe17a31d1caff1876cb94fbc4

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

MD5	4ba8d2b2b258e0570ea02cb704165ecb
SHA1	a5f423a5ec8d43af1a55e9f42b1677cd54c970b5
SHA256	4ae829dd113e794c8c9b393c90aac296d0fea9f6a9894fa226a7361c2ee4f205
SHA512	77a63974bf9c97fa9874767c3bdf96af7a47c7f8d8c563d53dc26b31d106741e9fca47ca6e9d102f7b6b789b4b19da79564e9a5b527ce16e2bbaaeefce0f9081

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

MD5	a2664cbcff5479035fd20385cf377069
SHA1	cac58190717bbcc53da4e5b2c73a4299c9fb6c72
SHA256	540c83e48c59bc2e057892affc3ef263d7832eb3db7a0c738f95f6619528fe2b
SHA512	d322c61a23a63d48a7dea329c0929daafcae8b55e0ecb124c6763b78703dc3f20b307f08f9669bfe0a56b6164ffd2db1f6324c39c8574a752b969190d0287c51

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

MD5	fa481888e0ac0b23b975070c83949d53
SHA1	3cafea946c5a5261d8970e0f22d3942791c10ed0
SHA256	230b801ff5d520e8b9aa9526c0b0f0d0333e6d46b9ae08498bad028eb8842e1e
SHA512	604fabb8f5848be51bc501b1fbfee8c351f38d01c7c2ce4b1470c9d74ac9bede5876fc92179453992c2f975b8b6e50d781680b32aa830789d95d54037b89a6b2

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\e4b7bc60-a708-4028-835b-b30156ed6388.tmp

MD5	5058f1af8388633f609cadb75a75dc9d
SHA1	3a52ce780950d4d969792a2559cd519d7ee8c727
SHA256	cdb4ee2aea69cc6a83331bbe96dc2caa9a299d21329efb0336fc02a82e1839a8
SHA512	0b61241d7c17bcbb1baee7094d14b7c451efecc7ffcbd92598a0f13d313cc9ebc2a07e61f007baf58fbf94ff9a8695bdd5cae7ce03bbf1e94e93613a00f25f21

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

MD5	7f4263c8d6bd1023078f4acec073e1b2
SHA1	93b2156e9b2516f9637ffd6106b18660a01153b2
SHA256	b5fba6320530923b1f869947f58f3b7f3e9375583f65488bd31fa2795952f6d7
SHA512	e6bae42a2a4305c24548f2567035431964a2a71cf96c92f71b5329d47d704285fd2a01804f1c85ee382de5f813eb36fa32d6e21097672d6b2c4ccc60a2b93063

memory/2940-4729-0x00007FFC014C0000-0x00007FFC014F4000-memory.dmp

memory/2940-4728-0x00007FF7BC120000-0x00007FF7BC218000-memory.dmp

memory/2940-4731-0x000001ED4FEE0000-0x000001ED4FEEC000-memory.dmp

memory/2940-4730-0x00007FFBEB330000-0x00007FFBEB5E6000-memory.dmp

memory/2940-4733-0x00007FFBE9840000-0x00007FFBE994E000-memory.dmp

memory/2940-4732-0x00007FFBEA070000-0x00007FFBEB120000-memory.dmp

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	a5555ca40160a35f3948e5f5a4265734
SHA1	5347a889885533eced0155d9030cec5ca47bd722
SHA256	3432cc83750af34d9637983f9fadefa85b1fdc055d59b5135037c630ee8b4f09
SHA512	ed3ceb8b7b72c75d37dd8abf6df8cf7d890864b19c0f87a5197012d3e07bd41bf188cbfa7379ac0a81a7c7ff0f70fe7fe06cbcc9895dc43a717bcac458dd473f

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

MD5	2eff7771510ec0b4c61b98fb80d71510
SHA1	6592c5bac521061ca129f77d709d10a8b1613573
SHA256	d68bb7132839b516f834f8a720b2f1b4e28bbd348b31b50fa5323b69c4866231
SHA512	94e7af37bb25b1d6537163f6623b8bb2553a0825eca673d5bd32d34c5ed1164403b265f0cbfce485f5124689abad48a5a1ef862a60f5c0d79c413a0375f3c415

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State

MD5	396e837ac599ae06429491a24177b421
SHA1	03707861ef596c8ac0323831a4edb5fa7eb9c7d4
SHA256	a737b4c1b93410399a3cdf26be6919d005331f1248650d4e295922c84faaf2f8
SHA512	119729362fd36d099d024cc7ff4b22f507206ab56f0fca453ec6c13cd7fac34164559d0cc6def97f6e185cadbd0745a42da80a44f17734fcec9efb0f83f36521

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

MD5	4db1c59fe3bf707621f53d5000d7971d
SHA1	a1a93224d7bc646fa3e311fff21f74317cbcb00e
SHA256	8ab0da0c2e30c37c366d8fe0d13b31724cf1080bd97e23daf39c8ce01def7f8f
SHA512	5d528054301034ca6f3de02ca24c2ed1ddfc1ab739ee8a43b506a985fc1bfc6281b0b0089b915eb0ed25aa84eec6920cc65da2b4a68b8da5e752392b4d57c690

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

MD5	77876caa86f52cb22288bbb11afdb954
SHA1	bffab8fc000dfd9cb7a709ce316ed2c663bc0613
SHA256	cf4d254df3375cbcb464073762d79c509459a860d585559da5f38de1be376ac0
SHA512	ca406731f6453062577a364819788a49a5c2d023c900677db079f8ef101055ac06a52eff2199344442cf0e62c97d2f5c95b1519a2905e4d963e67a3a358505e6

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

MD5	fa925c275e549bd8d48a088991c14257
SHA1	3671b3d4a036890d78ec5e602de166e836da005b
SHA256	c83df9a030d7afb7ed768313d42f0cf045eaf202692f004a1e04c4d7fc08a64d
SHA512	313c3cd62f8e82dcaa580e5d76d217a0bbd64a827bc0a7b5613ffc7470a167a7578aae42a61c5e043467b6a3b0f8dabc2a4daed83eb30db9e75b2c97c4705f76

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	7f143451439549ac2d99cdada0f845ad
SHA1	e25547a8aea0f9abe29557bf85d1765422bdaeb2
SHA256	07459fdcc2abaf8193759abf0dd9220992cc1f466a3643a5feadf2d06117bf7a
SHA512	e25be4e56d273a56a8ca8772b162cd049a0b46a3abe9edb809149066784bbc75fc6d0ed9fb68f17cf6a8d29a3c92b332525455a3d14aeb9254a4870776ca7f62

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	cd100d1a117b5db15976d6964cf22dd4
SHA1	055b6fca72f2c2a6f7d4762fac51b8fa1c38dcc0
SHA256	5aedf97dabf1588b35393474c98c1b8518468e16e3d9af7e2b65bf65afe04ce6
SHA512	8bad3380880da74d60f362fa48ec036ecefd05aad18521ac65fbbf875adb3191174516ecc8219cf578b38257d2009b0e0e9330b541e0fcb5257084158d4d7ae2

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

MD5	c87d016b22023ced6e3c89d586fef062
SHA1	6841acb3b8741df4353fd854777afaaf03dc238d
SHA256	b219da1ca33d46b317bf1907a2ce2488e2420bc951e06b73ecfb23fb0fcbe8bd
SHA512	80f90c6e8b7738e43e4c90604dc1745ec12c37e50cb1b6ff5498e5c9669e8d6892ea570cbc8187b265e623a70db39772b61a54d85598888d09ecb50fadbed681

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity

MD5	6a54dbba1616d11fe209d4572a01e9b4
SHA1	37d761e2057f8eedd54a6195d5f41d4664de1bd6
SHA256	1f0a8c630b927680d8cd20ba22cf859ba3e5d19adb3b3b53576e9d56a87b70fe
SHA512	62517313a64cf613dddd01d179c4cede4977abcbd2c24436d16e3a90280da9ecb591d2fdb3b00c334bb833fb0b996c13de93a6551ae96030d4ac7ec769e0f427

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	32f73214f40855e686bdc6a6ecae9065
SHA1	9f639d9fedcd5e34453ac8c349ae5c3044efbea7
SHA256	745a09d9ebe4fa89e21a42255eb62d74c3fe5e4a0468bc92b985b2694390e470
SHA512	830b741bf4237d373654fdfe9c219e4d80b3297408082a4f1e3e53cc6e53c26f4b12de1e407e1e23c808f260daf4af52cf9b6ff5fa052a2372d1272a273e2a83

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State

MD5	566293a2d3879f4b31086ac00f36715a
SHA1	07a73846f8b7808639b715b0cfc3b72eb811982d
SHA256	33240d6fe4ce1be47f94b73ec63399a9f138c7c76c6ff386877f140bbb3227b7
SHA512	187fa6bf18c8c74bf5132b31ed3ad6523a4bcd30ee99e43812880f30c1b83ab5e1f94477231c1ddd701dbe3c016d5f42d90e11dbe00698d5bdffe17d99bed9de

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

MD5	1fec82b778c478b83352a834b5a4dbcd
SHA1	0972ff1f0e8fa95420f3143c333391a2cea39706
SHA256	8e68657a23d3353bc3038d8d2911f631a96304fb109c0c6caa3c62b26cfa9fd4
SHA512	f660687252987274877607 73a04d7fbde43abbad124d0208882c2dfd3fa27eaadd64dd8f638caf742748064c2a81b0ed818f50f250b04495698af00c09147fe4

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

MD5	122cac69d9ad1e9e414a03288796d01a
SHA1	02026fa9857aa65c98011e01ad88fbf9a6e18a41
SHA256	7134ade44c1ddf0c89107a92b1216181db781f14d1f4b18e82773f5dd30fd626
SHA512	9f741e8a86b98d6451556c268ea9b043dce28dcbb378ee19b29df80285d2d8be7401e15fff5aa754a9292d84c0f3da251640f47af19f3dfb72e421534abb77d3

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_00002e

MD5	9a01b69183a9604ab3a439e388b30501
SHA1	8ed1d59003d0dbe6360481017b44665153665fbe
SHA256	20b535fa80c8189e3b87d1803038389960203a886d502bc2ef1857affc2f38d2
SHA512	0e6795255b6eea00b5403fd7e3b904d52776d49ac63a31c2778361262883697943aedcb29feee85694ba6f19eaa34dddb9a5bfe7118f4a25b4757e92c331feca

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	6934728a270ed01d58e6b90ae80b65fb
SHA1	311f4dc3db66d58c5586fc2f7dfcddd08ec1be59
SHA256	f78286ae44fdd7419a5cfab0b2f8ed69b5b84050d2860eafa60c63e8700091bc
SHA512	e6939e3528e5948305657ff8086d22bce7edc02d85ebd6029317f9a3a49f4e5bdcf9c56eeff4dade679955b259e521f1ce9f54cf03ae0ffc9f95ce3ae1ce931f

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	b15d061a42e429a197815e56de63ff68
SHA1	b4e1a76061f587d368dfd6a69def53578e9cd69f
SHA256	b322c52820edee85d4fd8ff760033515c55f26fe6c45d911b1959d08cb10e78b
SHA512	2bd40e4793178ea982359a49e76c4c63a10386ec8947fdd5adca2d209e5a67afc594b24292b0fc91de78ed6348e1728546ba77da4070299dd51525fb5371d23a

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

MD5	270dfa0f8c6b3e2f018e2b7f1a7fc22d
SHA1	33a3a267f25977951a1b50c69eb639385e1e6360
SHA256	41ba6f24c85cb1315cb743880649974c42b8ba1cc4967966e472adf814052bbb
SHA512	1438d26ba85f049238d6032422002788888bb68f7e6f95c70541ebb6bfb6459c0ba244e2bb66acb268cc67a1cb6b859dc821c529447a6a99b5243568cb919ff0f

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	c5b78d8d38b9f80d4d317657353b8630
SHA1	0d34ed489aba09a9077c202708ee54087d44aad8
SHA256	0975add3b0a0f6aa473546e38275a438af631b50ceb5320903dc61546bc27f02
SHA512	099af0a3b46f7008522efd9f4ee3430633a0312770b02bbf58bfc18232cb9635430477c3e700238c032978738f268c1d9d4f8fd61320b0572349a8b73029f59c

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\WebStorage\3\CacheStorage\index.txt

MD5	46cb7641be727eb4f17aff2342ae9017
SHA1	683a8d93c63cfa0ccbf444a20b42ae06e2c4b54d
SHA256	944fff1dd6764143550534f747243ef7d84fdac0642c94135ab40f584520f63e
SHA512	dc1b5f363e90abff5c1663a82764296922c842820d2819805e87da6da1081f1b5f2d8debc83ac34a26ce289b7b22588b022433686b19b039074ae184968b9fda

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\WebStorage\3\CacheStorage\index.txt~RFe60a24f.TMP

MD5	baf075dcb170d6cb397d77b82976f8a8
SHA1	60584c8ae0edfbd67ad9e25a9615f92ddbf002ed
SHA256	3f83bf345e10ad56fd0754b8930ad0f803055ef9251f515fde6704359f2c69df
SHA512	c76c178707f9d404af91f2574423ea92a944175d797e234d04fbba94ea910e269cc7d4ef8c2dba82f3a7d922b5c0385e9444100382bbf41d14b03e146b2758e6

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	ac99862b10606da1ff8db57c3cd220be
SHA1	50d629748d1cde3c305ce3a5a891f3ae9c63f87a
SHA256	127b6c6aff9b31c57162e9743a0ac2740790dd005a67bfa156ce4c23181dde5a
SHA512	7aa7633e6237d2b8884fb4a596f0a4562ce9bbe50d33615adaa21a66131174d3aceeb8e06a40723f93139252bc58739a4f715614b24bfaf454dac4d28e934b80

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	c55c8550036aa0c2858cf59e68d245fd
SHA1	a4a26568266cd020c9eebf40e29d2c1eeecb2ec7
SHA256	0305a4fe17cc1e9d3b9ca4eb0f438960f7666a6e4544b71d601be0b06e967e01
SHA512	7f1823bf9b2376929738c93cdb15c375acc9fb71b007575eae13cf6a47c8b84f976b6396cda4cf0fbc818258ac9fa5b45195c4ac17bb0429d17d77d964fa149a

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	94962c337ba8731412cc9a221a421ee3
SHA1	7ada77987fbdc7ce8938b30bfb329b574f894f75
SHA256	5822d31e3472498fac9d458e5dc9c26c1ed1f0916c7b604e83211ea4f8cf426c
SHA512	343f45656a6b58ceca01565346fd2808cece98cf611141bef581ed0252e30b1b18ceaecd687100295604c1663c49082c04d4bbaa160095e1f11d8bccc4e27de9

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State

MD5	4756b128be0df70fd4d5b80d1cbfcc1a
SHA1	73afefad7a4f87f7a590b22b0d67d87345e5c562
SHA256	c85cb1be1e4e718ed0bf6ec493845b8af01515637fef7616c6a19b06db536748
SHA512	12f564165158d39a74d476212cec1a1cfb23edd059242297e991932c390c64691cd3b8bad38f39d5ac39d543fd642673a69fae08e85543b67b2415726309b945

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	b076ce3190572ae8f0a154a4444b122c
SHA1	d6fcb84615a06f7ad73a6750869c67e94ad5f6cf
SHA256	330f4b4642f6c7f1d212a309fdf0cc294c7bf7365c5e4a3e6457623cc765ec97
SHA512	fe66baf4f7edadf9a4f14d1d4155eb9d4e4b9822cbd150be64bde23e68a69afe340c9c1b932cbda12673ca895cd8af967d2ec4e6d168e2e157206f4704dda81a

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State

MD5	271cf095148befd2eb656e99acdcae72
SHA1	14e6f52026d285fe3fbf4427f45b8f61b3afa07a
SHA256	da2a1c8693875c9aee780d9d27c5a961c9ccaa6062e2cd2eb2f877acbfa5fb00
SHA512	fae734b4c4509d10f3a67df99b5b03e93be9543d15d2d9620aa8919a4c90a98cff978c4c62793d90b014cf3a423b90591dd1def7d39968bdb12e1a411f0294fc

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	050b3af6d6832939df18656d825e745a
SHA1	070aa6ed633ab7b1d79d30fdf46548f8b552de0a
SHA256	45049f6713a19f14b6a6d7e9197068cb08a92e1411bc03509bbc14ce83ff5afa
SHA512	b5fe7348321c466edae4cf5c28d22c703264b75114f3f7191e15eb5742f59f3051d14f600df4342023df767e075a143278dee9d5925bbba86e9d4d60b9c19d2b

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\WebStorage\3\CacheStorage\index.txt

MD5	f8ad52f52098e9c71a89dda7d78dd4a7
SHA1	3af2d2534fb9cdb095faf25ab6882eac498591bb
SHA256	8cfebcffc7b21722cdce34493040fc258e1ca65aab4fa00712d0251c4d0ba117
SHA512	25da828960740028365 82d19e9a96ecdb7b59a5a392689539fe5ce7b403f92d07f04a70652c2b8266aeea2a653ad2d1a008cd17a04c4a0534f50e36b42bd24d6

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	24b17e028fe81d1f83d1a683d03f8645
SHA1	f992217da56bd31603350643abf099fb41e1c0ab
SHA256	a95ffa985610f2e568e94ff8d917d877d2bff46f1474a2dc674dde448628b58f
SHA512	369605d4ad011dab88e1b7ea0ca903c2645d8128caa7a66283c33c2342a9a091c73bdee9e782b878b550299ee0dc2dd56afd263234449a3bf91585adc5d5c143

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	89f53e78049e2212a356232ecf20cd7c
SHA1	4a625fd91c0f05c59f9f2eaa7fc2f91cc5d73a01
SHA256	be5ec461eb301a854fae19e04e2125069f68d184cb8113db9781fdfd0174c9f6
SHA512	6aa1d1832f6a7a37236af5fe4f0e8bb48d571d420ba67fcbad5b799dfd47ad948957672fcd17512f2883c7af331e2e4b72db15ba4c160a1be3c32fd8dea0d6a0

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\WebStorage\3\CacheStorage\index.txt

MD5	f8ae1af1b356810eb68ef9610cbf0a04
SHA1	72d2bf45d3cb89dacd00aa2f0d9e089e0d9b4b39
SHA256	1856483f82aef0177728891ae9d97f625adc74d2d1333b9c6538c6bd37398ee4
SHA512	fee5081be2aec2304dbcb5116d0e9177445f11a0269e4b5843540c8722304a2a3c51c032a39c1df7efa5f91b274433f95a50a7599ca17e1cf00ed215876eedb0

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	ac88f2fdd060c7331bb669429c154224
SHA1	65f9e4816c74926e5623084fb917521a1aa00d5f
SHA256	c20d46a35aadfc00250776d8d456f47aea14e404b2b6325144e10378598b1cf6
SHA512	d7066794264c65ce18b2a01695a4df2834b61c2280372a796d3ea4f661dc43e8bd4b0fea35c6de3694b4bfec045c262f1062f111c94848f2ccd106663c0f85ab

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000042

MD5	e89110ed8502fcaffb3ac220bca7acc9
SHA1	18e3adba01f2ea8d4bf55a6509175843fff6947d
SHA256	2e6ad719c867e021bfc32baa9bc78330ac531e6bd76dad0dbfabb860ff330b81
SHA512	9ab0380b86a8f2abc47015bff560db0c759eab25780718f6913d71116e31bf4c28f750cbf39cfb7ef194c7efd2cbaa0830c6c662b7b0649e0d13f83079d1c0ea

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000043

MD5	86b720c908fd473da7f0eb0a9a9daf22
SHA1	24fc84fd3aea224ea0656be3f943edcf7ce4a1e9
SHA256	82727a04eadb3c4be02cee4a1e6020bb2859e650238072ced690a336d418ce60
SHA512	8ae8f91904f6071767f949d48755fe9a3663c28a8cf67d41521f861183d49cf2e03eedc6523906dfdb9b8776229c3039719034ba8aed7d8d18c9882ec8a1197e

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Shared Dictionary\cache\index-dir\the-real-index

MD5	f29b1eef915ec7f7b08745b6eab74039
SHA1	0e62c1615bb7aee530006ad1c6ad5188f7ffd0e6
SHA256	364344754c7da75673e6ddda527b01147216d127067671b6549f5743033fc142
SHA512	ffb6363e7d716d7ffe4f1a8a384dda889758a19932e4af56a06b73e14a572a17398408d271126ce513bfd1aef52f180e717b8b2e5add5adae0ef52a489dba574

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000046

MD5	761ea31dab0e7cbcdf7772b193b452fc
SHA1	511db2b8e52899ec9bba1034663941d7df1bc868
SHA256	4e361122da79d815c1bb8845e381d209e704ccf027cde0f84abe47261bcc278c
SHA512	6436618b226d2e4092488127647c6d2b9c69b66a5b81e778cad5cd0006dd35495ef5304d2c0c5f31b55dedfbfb944b55d3eff7740761129e1612d08f29bc220b

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\f_000065

MD5	bd6b6871c752f166af7495444c30a04d
SHA1	38807538e870b894cdefc1c4e82716a0231da0f6
SHA256	6bacce1463ac1df0739bd6ce91c835d768c7bc2154193728e425d4861c82a01b
SHA512	a27a07436208d17734e190988484e31ccc5263e613db249797ee6e18a39c3965a17e07883759c2766ca89956d98da12417d13e5318c0e2345a1a09b6e9f7c3ae

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State

MD5	64857fc3df72ee985c9e5830d42f3d24
SHA1	066fed399695102a20b55b1893494dfb3ac0bd91
SHA256	ea0eef530ab04a0388aa60a88ca0676a4522b928e3aae4b603c0d5bfe1151252
SHA512	652316ae5ad2f7bdf65e137edbc4049e911b16e48694764f6d5810c95699c01283c423fdf3a77e98c7a76525e29d1e529a61b53f06d27e304f1b059d30b5b6ab

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	b4fe8ecaf5a5aa0ab714941f91ca891f
SHA1	bb1490a18e3545a4de1fbefd074259bf2a233508
SHA256	7c7442f0a811ba486bd1d7bce5052744dccef42d8467041d1171154853b30141
SHA512	df12294afb4185ee4eacbca558ec4bd2c60e9fc7e3183c4e80f4f2b6d7f1867eec3cb3069133e6c54beb5158217d37d1d8f8b62b8469c65a802b5b07bacd22d9

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	304217618e8443b8cc3bd699431a59f7
SHA1	73a77c624d76f7a0fde52cfc12330ebb31ce4902
SHA256	f3b07fd15f18fe21922ac3db96a0bcae347a336047d9b526cd2dc1c1bf5c7a5a
SHA512	48cad38b07773b074eb9cddea96a9448e78a77da9a1e3684826f446c2092649b3af6c966b8c4677cfd619f82b7c6e9b33eb34cfc9751e1c7fe11cbc38150fb60

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

MD5	089224588ac9066611aafc94fbbc0c88
SHA1	1491c773302d4c06078debabf19a2f8b30d86f19
SHA256	925afa140d392d81266076ec172df9bd7b14fab8c409840c89e381207203d56a
SHA512	a9fc671e2ebdd42ef216ce2a6232d953f9113683dfde7c288b6ab01a5e638609029475c21bfc34733c8817293ff91a29d466fec34ef47c5fc036e522bcae2eaa

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

MD5	9e920fb026b4e566ac9d4ff683d203b8
SHA1	78b3af37b8ef9c23eded1923fa3714049a4bbf7c
SHA256	38de41634b159d43159edc9ee95a8cd18bb83f76685364a4c76fb479e13f6cd6
SHA512	ae477f89ae8cb199ea3cbed4b46b94cabb43ecdc93420d14e9aa0f879b68da5d551b1d09bb24e150d6b74a3774f16904a211315f9664ade99bb5cabf5aace9eb

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State

MD5	fbd4a608d0d2c53ce880bcb6d49df12b
SHA1	8e280a6d3f2ef45d9fd021653000ca63c5acded7
SHA256	a4429377d22930a0dafda664aec3a1d37bd1cb3879b642099e652726019af630
SHA512	7cc229dce00b7b204dabe36d67d7a09cc5195c76a56832b93264dea6b2cf09ca9c5ca44bb535f572ac697f38fc69af9892d3ce6918f2fbfc653c5df8150e276f

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\WebStorage\3\IndexedDB\indexeddb.leveldb\LOG

MD5	6d090c245376a34a5d2d69194cdc9367
SHA1	52becd3a88ce2d9b9a591270a0c08201a268d6fd
SHA256	e95e9ffe3f4a70b614a28354339f29d782591b0e3dc5bee62bde55cbe9541b6b
SHA512	86dac6b249e92dfeb45fc1074df8b84f77ea3ed29d9869fcd57f23ada085d141c20920b70a8d95686169cb09ca6142eac925c0d4fe3f063fce5e9487bfdc0a21

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\WebStorage\3\IndexedDB\indexeddb.leveldb\000003.log

MD5	6834bdbd9f2de7e2a26621815a0594f7
SHA1	5024806aea946c6febfccbf86b47179eb907d5ce
SHA256	e28fc40e5eb6910ba649bb67ff4ffa779076fb6298e5b47dc02c8deb2b770f7a
SHA512	92dbab7fc6639d1b21c497090220011212caf1ab58bebd31b982b0fcc07738f49e00f43e1ac1fe8460a8fdc02e36febb587415ae05327f0c134cd100d26fd4de

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Network\Network Persistent State

MD5	728f285ca3d93d3c8a533f028842de4c
SHA1	662e2a7adfc244740c8d47c5f89fe90d82e56862
SHA256	c3b6838d470e3343b74af283fe1c703d575ea330b70f757dbaa5474b14da14d8
SHA512	e73f6df1876f6fbb1fe2e5c319ff7fb9db55ac43c2fdf3c1b79523437f808ca3e44e18d1eea4ea7922fd34a1ac4bde02d9bf541d170c03f40b0db2f2c28f21e3

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Local State

MD5	92611ce2d8a16dd63d83d93254a2acfe
SHA1	8646757a6489d410907455edb02244d73bbc20ba
SHA256	afb403626364b3e4e330f4fa2f8859e38635c8ca342fec2aa6d0c33548de8ab3
SHA512	ae24598a759b7e4c62a8519383ecb0dc6fa589d3e1e96adb3a91c5dcfec879f5f90b0ffdea62075d461f2a115431db4bd005d0be6626a3e0a6e68c3b3546572b

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	844fbf59b0985917a32d8dcbe7a7b77f
SHA1	d0a547d90776e59a8f5ca1b911bc7fc6674bbe07
SHA256	57c2ac662b08c23355671d55065997879b0e7a33a12c9a789e24decc0f8dbb67
SHA512	bd16d2de49f647608b4939d05ab9f21da2cbbd11caeaaedacfcc8b9b1f37d195b0cd07baf21714d68be4f4efd3b80ad7b7cc542e1b62870f6e50a9a453a908ab

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e823f6beb81f1f87_0

MD5	42c7e730b46ea58e5b694d80be0b2d86
SHA1	57d16bf50e82d11aff70485986a210b66e30983b
SHA256	3fcf005fc56a2aa4721a8b69652bb6054252c41b38775909eb2cf389b2bc1110
SHA512	a1fa2d0a9c670f94fee7d665d8a14a2ebd8fb572d822f7c0aba6872b54e607e3496945af7aec89deb72db465c4706ca60224bffe901bc5be2783e391be9f3516

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2dbaae449464b96e_0

MD5	09687c1fa0c78eee845c2f51b6ec8448
SHA1	089d8e1a16a26d292596035404b3c47ca7a7364c
SHA256	46fa77cbdde8fe3ac08c9bce6a708e2ffeba87c1e9da320ba36c0312814123d6
SHA512	f5a3068d5e5f6d2398ba51ef9cb8ad60aac4e878e08cd48632e009cea72997c078d93d810b522f2f43e8af43e44c9087a7032ff21a35f2c0f98cb9f6783ffbb1

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c41ef0b705049e03_0

MD5	bc7b144a3963c2f5c26e1fa25da6ecbb
SHA1	f7b9ceede83ec0aa2645dec08119dd502acbc9e3
SHA256	404a786cfceee5076adefc7dff643072f99224a989bd6e235cab3de4fc018c62
SHA512	f9c9ccb88555c750b568abe7dea1b66a496b7e1b3068a944f42d7bcbb2f1f88dbe4f1ec459860b7a8e1c4dc01893c084b5620187d8019a6c1614513dfe1c3e66

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e2ec98e43301f05e_0

MD5	06ff2fdfe1929bbe42656cda4b56f24d
SHA1	8290eef7307718d8d3ab7aa6986f25138ff29769
SHA256	5ea6f43191af9b6bc7dbae0e0833748add3da8d5235a6132482553358084e86b
SHA512	2e29eb2d71bdfaa07551bf71e49dbf79de0aeaeb798fbf6110fccde4463c3e4558c481ae2bf27fd5017124092b515be8883c10aea6c4cad2427d88b5e0406513

C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\Preferences

MD5	96b83bb65ea0ebffdfde4f39882b125b
SHA1	3ce264e2678b00df3d9aeea19fa875d09d8e0255
SHA256	aef1f3b76efc762083daf10bb2490357aff181cec87c8b65d483342440e9a869
SHA512	76e978108bdb2049cac8c2044b676b47f73588422d8772b208a543e8410e5cb228b26f6910514117fc2475b3b99a12eb73bddf28d23a81b2f53f35ed3b4dc4b1