ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

URL: smartonestartpdf.com

Full analysis: https://app.any.run/tasks/a969af83-94b6-4f6e-bd0f-3339e4bd452a

Verdict: Malicious activity

Threats:

Adware

Adware is a form of malware that targets users with unwanted advertisements, often disrupting their browsing experience. It typically infiltrates systems through software bundling, malicious websites, or deceptive downloads. Once installed, it may track user activity, collect sensitive data, and display intrusive ads, including pop-ups or banners. Some advanced adware variants can bypass security measures and establish persistence on devices, making removal challenging. Additionally, adware can create vulnerabilities that other malware can exploit, posing a significant risk to user privacy and system security.

Loader

A loader is malicious software that infiltrates devices to deliver malicious payloads. This malware is capable of infecting victims' computers, analyzing their system information, and installing other types of threats, such as trojans or stealers. Criminals usually deliver loaders through phishing emails and links by relying on social engineering to trick users into downloading and running their executables. Loaders employ advanced evasion and persistence tactics to avoid detection.

Stealer

Stealers are a group of malicious software that are intended for gaining unauthorized access to users' information and transferring it to the attacker. The stealer malware category includes various types of programs that focus on their particular kind of data, including files, passwords, and cryptocurrency. Stealers are capable of spying on their targets by recording their keystrokes and taking screenshots. This type of malware is primarily distributed as part of phishing campaigns.

Analysis date: March 07, 2025 at 01:07:09

OS: Windows 10 Professional (build: 19045, 64 bit)

Tags: adware advancedinstaller loader stealer

Indicators:

MD5: 5C5D1D563043ECD13621ECCC05ADE24D

SHA1: A3A0BA2C7B4029EFBF9B2166E95F2C2022E1C6F9

SHA256: E309D5127E148557327C8B23455DCF2787D48A1B616FBE92F37FF9D4DBE65D3B

SSDEEP: 3:GRAaBdI:GAJ

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	**Heavy Evasion option:**	off	**Network geolocation:**	off
Additional time used:	240 seconds	**MITM proxy:**	off	**Privacy:**	Public submission
Fakenet option:	off	**Route via Tor:**	off	**Autoconfirmation of UAC:**	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)
- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)

Hotfixes

- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- QuickAssist Package
- RollupFix
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- TabletPCMath Package
- UserExperience Desktop Package
- WordPad FoD Package

Behavior activities

MALICIOUS

Executing a file with an untrusted certificate
- onestart_installer.exe (PID: 9076)
- setup.exe (PID: 7740)
- setup.exe (PID: 7932)
- setup.exe (PID: 8648)
- setup.exe (PID: 8352)
- onestart.exe (PID: 1280)
- onestart.exe (PID: 7780)
- onestart.exe (PID: 7748)
- onestart.exe (PID: 4652)
- onestart.exe (PID: 3192)
- onestart.exe (PID: 7148)
- onestart.exe (PID: 9132)
- onestart.exe (PID: 5972)
- onestart.exe (PID: 900)
- onestart.exe (PID: 3012)
- onestart.exe (PID: 8776)
- onestart.exe (PID: 4932)
- onestart.exe (PID: 7596)
- onestart.exe (PID: 7736)
- onestart.exe (PID: 8632)
- onestart.exe (PID: 8360)
- onestart.exe (PID: 8668)
- onestart.exe (PID: 8436)
- onestart.exe (PID: 4300)
- onestart.exe (PID: 6512)
- onestart.exe (PID: 8912)
- onestart.exe (PID: 8712)
- onestart.exe (PID: 5984)
- onestart.exe (PID: 8868)
- onestart.exe (PID: 9008)
- onestart.exe (PID: 856)
- onestart.exe (PID: 1852)
- onestart.exe (PID: 6724)
- onestart.exe (PID: 1532)
- onestart.exe (PID: 8696)
- onestart.exe (PID: 8472)
- onestart.exe (PID: 5380)
- onestart.exe (PID: 1600)
- onestart.exe (PID: 3396)
- onestart.exe (PID: 8080)
- onestart.exe (PID: 540)
- onestart.exe (PID: 4464)
- onestart.exe (PID: 8748)
- onestart.exe (PID: 896)
- onestart.exe (PID: 7932)
- onestart.exe (PID: 6392)
- onestart.exe (PID: 9096)
- onestart.exe (PID: 7940)
- onestart.exe (PID: 8372)
- onestart.exe (PID: 8352)

ADVANCEDINSTALLER has been detected (SURICATA)
- msiexec.exe (PID: 8948)

Connects to the CnC server
- onestart_installer.exe (PID: 9076)
- onestart.exe (PID: 1280)

ADWARE has been detected (SURICATA)
- onestart_installer.exe (PID: 9076)
- onestart.exe (PID: 1280)

Actions looks like stealing of personal data
- notification_helper.exe (PID: 2392)

Changes the autorun value in the registry
- onestart.exe (PID: 1280)

SUSPICIOUS

Executes as Windows Service
- VSSVC.exe (PID: 9060)

Reads the Windows owner or organization settings
- msiexec.exe (PID: 8852)

Access to an unwanted program domain was detected
- msiexec.exe (PID: 8948)
- onestart_installer.exe (PID: 9076)
- onestart.exe (PID: 1280)

Reads security settings of Internet Explorer
- msiexec.exe (PID: 8948)
- msiexec.exe (PID: 8916)
- ShellExperienceHost.exe (PID: 6736)

Potential Corporate Privacy Violation
- msiexec.exe (PID: 8948)

Process requests binary or script from the Internet
- msiexec.exe (PID: 8948)

Application launched itself
- setup.exe (PID: 7740)
- setup.exe (PID: 8648)
- onestart.exe (PID: 1280)
- onestart.exe (PID: 8696)
- onestart.exe (PID: 8472)

Executable content was dropped or overwritten
- onestart_installer.exe (PID: 9076)
- setup.exe (PID: 7740)
- onestart.exe (PID: 8668)

Creates a software uninstall entry
- setup.exe (PID: 7740)

Searches for installed software
- setup.exe (PID: 7740)

The process deletes folder without confirmation
- msiexec.exe (PID: 8916)

Starts CMD.EXE for commands execution
- msiexec.exe (PID: 8916)

The process checks if it is being run in the virtual environment
- onestart.exe (PID: 1280)

INFO

Reads Environment values
- identity_helper.exe (PID: 5544)
- msiexec.exe (PID: 8916)
- msiexec.exe (PID: 8948)

Checks supported languages
- identity_helper.exe (PID: 5544)
- msiexec.exe (PID: 8916)
- msiexec.exe (PID: 8852)
- msiexec.exe (PID: 8948)
- onestart_installer.exe (PID: 9076)
- setup.exe (PID: 7740)
- setup.exe (PID: 7932)
- notification_helper.exe (PID: 2392)
- onestart.exe (PID: 1280)
- setup.exe (PID: 8352)
- onestart.exe (PID: 7780)
- setup.exe (PID: 8648)
- onestart.exe (PID: 7748)
- onestart.exe (PID: 4652)
- onestart.exe (PID: 3192)
- onestart.exe (PID: 3012)
- onestart.exe (PID: 5972)
- onestart.exe (PID: 7148)
- onestart.exe (PID: 4932)
- onestart.exe (PID: 8776)
- onestart.exe (PID: 7736)
- onestart.exe (PID: 900)
- onestart.exe (PID: 9132)
- onestart.exe (PID: 7596)
- onestart.exe (PID: 8632)
- onestart.exe (PID: 6512)
- onestart.exe (PID: 8360)
- onestart.exe (PID: 8436)
- onestart.exe (PID: 8712)
- onestart.exe (PID: 4300)
- onestart.exe (PID: 8912)
- onestart.exe (PID: 8668)
- onestart.exe (PID: 5984)
- onestart.exe (PID: 8868)
- onestart.exe (PID: 856)
- onestart.exe (PID: 9008)
- onestart.exe (PID: 6724)
- onestart.exe (PID: 1852)
- onestart.exe (PID: 1532)
- onestart.exe (PID: 8080)
- onestart.exe (PID: 8696)
- onestart.exe (PID: 8472)
- onestart.exe (PID: 5380)
- onestart.exe (PID: 1600)
- onestart.exe (PID: 8748)
- onestart.exe (PID: 4464)
- onestart.exe (PID: 896)
- onestart.exe (PID: 3396)
- onestart.exe (PID: 540)
- onestart.exe (PID: 9096)
- onestart.exe (PID: 7932)
- onestart.exe (PID: 6392)
- onestart.exe (PID: 8352)
- onestart.exe (PID: 8372)
- onestart.exe (PID: 7940)
- ShellExperienceHost.exe (PID: 6736)

Executable content was dropped or overwritten
- msedge.exe (PID: 7320)
- msedge.exe (PID: 3956)
- msiexec.exe (PID: 8804)
- msiexec.exe (PID: 8852)

Reads the computer name
- identity_helper.exe (PID: 5544)
- msiexec.exe (PID: 8852)
- msiexec.exe (PID: 8916)
- msiexec.exe (PID: 8948)
- onestart_installer.exe (PID: 9076)
- setup.exe (PID: 7740)
- notification_helper.exe (PID: 2392)
- setup.exe (PID: 8648)
- onestart.exe (PID: 1280)
- onestart.exe (PID: 4652)
- onestart.exe (PID: 7748)

- onestart.exe (PID: 3012)
- onestart.exe (PID: 7736)
- onestart.exe (PID: 8472)
- onestart.exe (PID: 8696)
- ShellExperienceHost.exe (PID: 6736)

Application launched itself
- msedge.exe (PID: 3956)

Checks proxy server information
- BackgroundTransferHost.exe (PID: 9004)
- msiexec.exe (PID: 8948)
- onestart.exe (PID: 1280)
- slui.exe (PID: 7744)

Reads security settings of Internet Explorer
- BackgroundTransferHost.exe (PID: 8732)
- BackgroundTransferHost.exe (PID: 9004)
- msiexec.exe (PID: 8804)
- BackgroundTransferHost.exe (PID: 8264)
- BackgroundTransferHost.exe (PID: 8544)
- BackgroundTransferHost.exe (PID: 9200)

Reads Microsoft Office registry keys
- msedge.exe (PID: 3956)

Reads the software policy settings
- BackgroundTransferHost.exe (PID: 9004)
- msiexec.exe (PID: 8804)
- msiexec.exe (PID: 8852)
- slui.exe (PID: 7900)
- slui.exe (PID: 7744)

Creates files or folders in the user directory
- BackgroundTransferHost.exe (PID: 9004)
- msiexec.exe (PID: 8948)
- onestart_installer.exe (PID: 9076)
- setup.exe (PID: 7740)
- notification_helper.exe (PID: 2392)
- setup.exe (PID: 8648)
- onestart.exe (PID: 1280)
- onestart.exe (PID: 4652)

Manages system restore points
- SrTasks.exe (PID: 8528)

The sample compiled with english language support
- msiexec.exe (PID: 8804)
- msiexec.exe (PID: 8852)
- msiexec.exe (PID: 8948)
- onestart_installer.exe (PID: 9076)
- setup.exe (PID: 7740)
- onestart.exe (PID: 8668)

Reads the machine GUID from the registry
- msiexec.exe (PID: 8852)
- onestart.exe (PID: 1280)

Process checks computer location settings
- msiexec.exe (PID: 8916)
- onestart.exe (PID: 1280)
- onestart.exe (PID: 5972)
- onestart.exe (PID: 7148)
- onestart.exe (PID: 9132)
- onestart.exe (PID: 900)
- onestart.exe (PID: 8712)
- onestart.exe (PID: 5380)
- onestart.exe (PID: 3396)
- onestart.exe (PID: 1600)
- onestart.exe (PID: 4464)
- onestart.exe (PID: 896)
- onestart.exe (PID: 8748)
- onestart.exe (PID: 540)

Create files in a temporary directory
- onestart.exe (PID: 1280)

Manual execution by a user
- onestart.exe (PID: 8696)

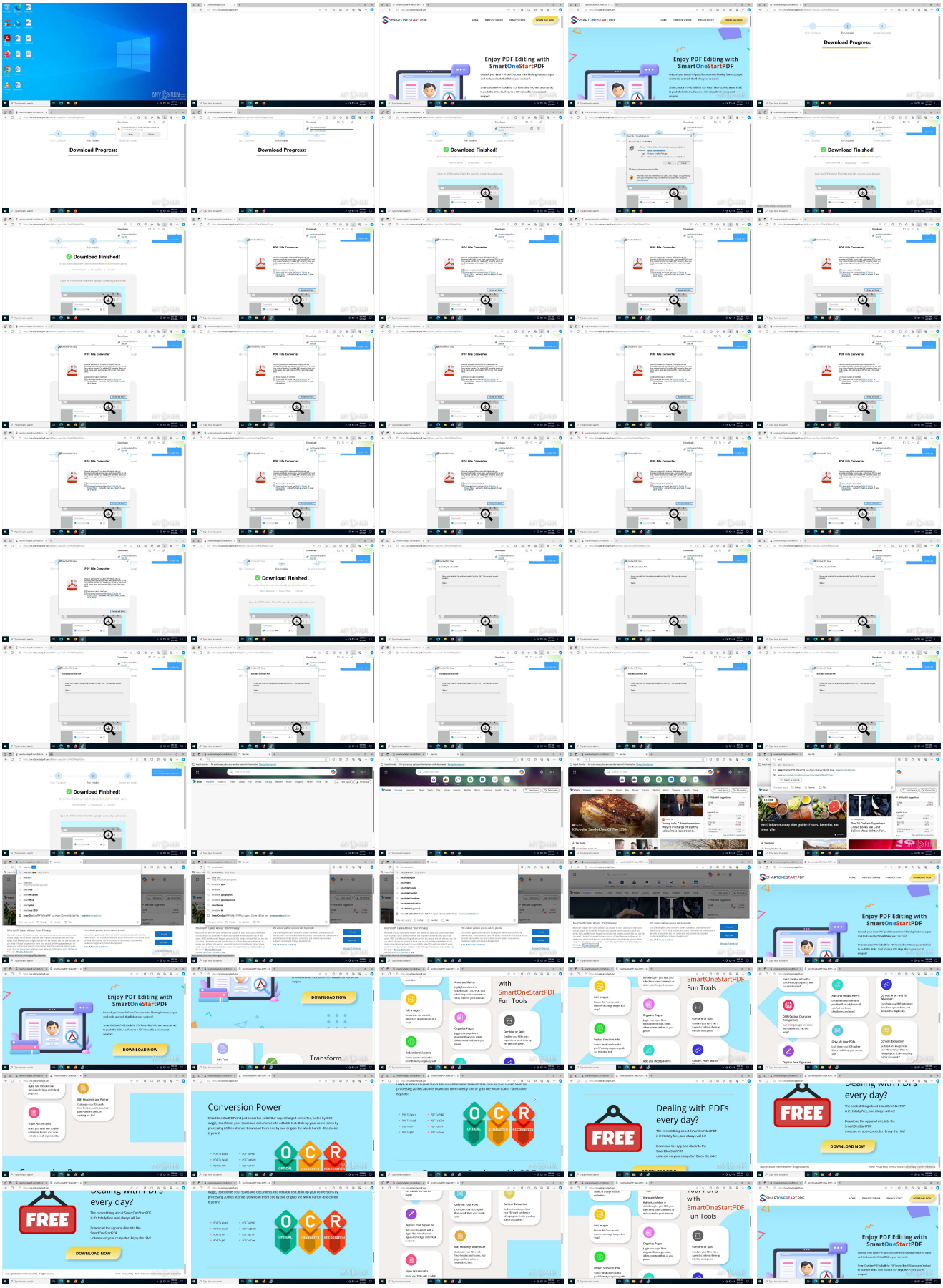
Malware configuration

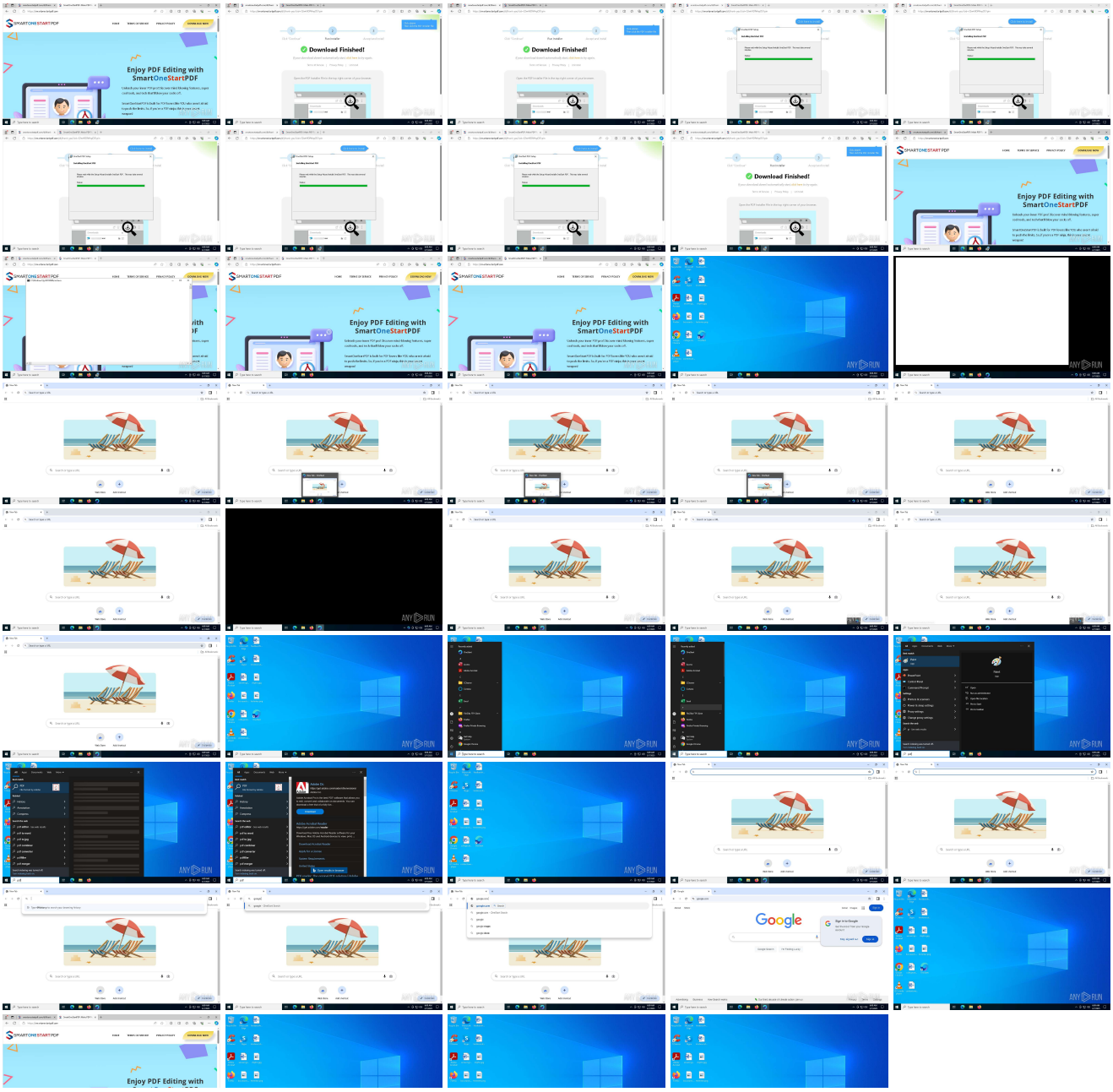
No Malware configuration.

Static information

No data.

Video and screenshots

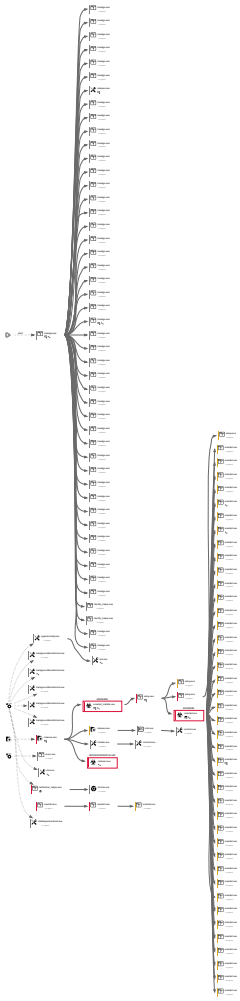



Enjoy PDF Editing with SmartOneStartPDF
Download Finished!
Google

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
268	118	9	45

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
3956	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" "smartonestartpdf.com"	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		explorer.exe

Information

User:	admin	**Company:**	Microsoft Corporation

PID	CMD	Path	Indicators	Parent process

Integrity Level: MEDIUM **Description:** Microsoft Edge
Version: 122.0.2365.59

2908	"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=122.0.6261.70 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 "--annotation=prod=Microsoft Edge" --annotation=ver=122.0.2365.59 --initial-client-data=0x314,0x318,0x31c,0x30c,0x324,0x7ffc887e5fd8,0x7ffc887e5fe4,0x7ffc887e5ff0	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: MEDIUM **Description:** Microsoft Edge
Version: 122.0.2365.59

7312	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=2308 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:2	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge
Version: 122.0.2365.59

7320	"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-appcompat-clear --mojo-platform-channel-handle=2420 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:3	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: MEDIUM **Description:** Microsoft Edge
Version: 122.0.2365.59

7344	"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-appcompat-clear --mojo-platform-channel-handle=2640 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge
Version: 122.0.2365.59

7580	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=6 --mojo-platform-channel-handle=3460 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge
Version: 122.0.2365.59

7604	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --mojo-platform-channel-handle=3616 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge

PID	CMD	Path	Indicators	Parent process

Exit code: 0 **Version:** 122.0.2365.59

7736	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=renderer --extension-process --renderer-sub-type=extension --no-appcompat-clear --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=7 --mojo-platform-channel-handle=4040 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:2	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge
Exit code: 0 **Version:** 122.0.2365.59

7744	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=4324 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge
Exit code: 0 **Version:** 122.0.2365.59

7836	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=9 --mojo-platform-channel-handle=5196 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge
Version: 122.0.2365.59

8108	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=3452 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge
Exit code: 0 **Version:** 122.0.2365.59

8116	"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 --no-appcompat-clear --mojo-platform-channel-handle=3828 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge
Version: 122.0.2365.59

8124	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5400 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: LOW **Description:** Microsoft Edge
Exit code: 0 **Version:** 122.0.2365.59

8132	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

PID	CMD	Path	Indicators	Parent process
	--service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5456 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8			

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

7620	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5736 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

7992	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5752 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

7872	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5600 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

7800	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5940 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

7792	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=18 --mojo-platform-channel-handle=4608 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

7868	C:\WINDOWS\system32\SppExtComObj.exe -Embedding	C:\Windows\System32\SppExtComObj.Exe	—	svchost.exe

Information

User:	NETWORK SERVICE	Company:	Microsoft Corporation
Integrity Level:	SYSTEM	Description:	KMS Connection Broker
Exit code:	0	Version:	10.0.19041.3996 (WinBuild.160101.0800)

PID	CMD	Path	Indicators	Parent process
7900	"C:\WINDOWS\System32\SLUI.exe" RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Action=AutoActivate;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=4de7cb65-cdf1-4de9-8ae8-e3cce27b9f2c;NotificationInterval=1440;Trigger=TimerEvent	C:\Windows\System32\slui.exe		SppExtComObj.Exe
2148	"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 --no-appcompat-clear --mojo-platform-channel-handle=5664 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
4040	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=20 --mojo-platform-channel-handle=5692 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
664	"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 --no-appcompat-clear --mojo-platform-channel-handle=6012 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
8100	"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 --no-appcompat-clear --mojo-platform-channel-handle=6408 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
4920	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6708 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
4000	"C:\Program Files (x86)\Microsoft\Edge\Application\122.0.2365.59\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=6832 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\122.0.2365.59\identity_helper.exe	—	msedge.exe

Information

User:	NETWORK SERVICE	**Company:**	Microsoft Corporation
Integrity Level:	SYSTEM	**Description:**	Windows Activation Client
Exit code:	1	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	122.0.2365.59

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Version:	122.0.2365.59		

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	122.0.2365.59

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	122.0.2365.59

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	122.0.2365.59

PID	CMD	Path	Indicators	Parent process

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	PWA Identity Proxy Host
Exit code:	3221226029	Version:	122.0.2365.59

5544	"C:\Program Files (x86)\Microsoft\Edge\Application \122.0.2365.59\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=6832 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application \122.0.2365.59\identity_helper.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	PWA Identity Proxy Host
Exit code:	0	Version:	122.0.2365.59

8200	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=7104 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

8240	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=7272 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

8320	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=7112 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

8328	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=7252 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

8336	"C:\Program Files (x86)\Microsoft\Edge\Application \msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=7080 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

PID	CMD	Path	Indicators	Parent process
8452	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=quarantine.mojom.Quarantine --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=5932 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

8532	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6176 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

8616	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=7244 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

8732	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	—	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

9004	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	↔	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

9200	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	—	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

8264	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	—	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

8544	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	C:\Windows\System32\BackgroundTransferHost.exe	—	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Download/Upload Host
Exit code:	1	Version:	10.0.19041.3636 (WinBuild.160101.0800)

PID	CMD	Path	Indicators	Parent process
8804	"C:\WINDOWS\System32\msiexec.exe" /i "C:\Users\admin\Downloads\smartonestartpdf.msi"	C:\Windows\System32\msiexec.exe		msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows® installer
Exit code:	0	Version:	5.0.19041.1 (WinBuild.160101.0800)

PID	CMD	Path	Indicators	Parent process
8852	C:\WINDOWS\system32\msiexec.exe /V	C:\Windows\System32\msiexec.exe		services.exe

Information

User:	SYSTEM	Company:	Microsoft Corporation
Integrity Level:	SYSTEM	Description:	Windows® installer
Version:	5.0.19041.1 (WinBuild.160101.0800)		

PID	CMD	Path	Indicators	Parent process
8916	C:\Windows\syswow64\MsiExec.exe -Embedding BFB89E44CECE2AB6F95ED30A0508DCAF C	C:\Windows\SysWOW64\msiexec.exe	—	msiexec.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows® installer
Exit code:	0	Version:	5.0.19041.3636 (WinBuild.160101.0800)

PID	CMD	Path	Indicators	Parent process
7808	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=7972 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

PID	CMD	Path	Indicators	Parent process
6712	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=7520 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

PID	CMD	Path	Indicators	Parent process
1532	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=4368 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

PID	CMD	Path	Indicators	Parent process
9060	C:\WINDOWS\system32\vssvc.exe	C:\Windows\System32\VSSVC.exe	—	services.exe

Information

User:	SYSTEM	Company:	Microsoft Corporation
Integrity Level:	SYSTEM	Description:	Microsoft® Volume Shadow Copy Service
Version:	10.0.19041.1 (WinBuild.160101.0800)		

PID	CMD	Path	Indicators	Parent process
9212	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --instant-process --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=36 --mojo-platform-channel-handle=6032 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation

PID	CMD	Path	Indicators	Parent process
	Integrity Level: LOW **Description:** Microsoft Edge **Version:** 122.0.2365.59			
8384	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=3808 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
	Information **User:** admin **Company:** Microsoft Corporation **Integrity Level:** LOW **Description:** Microsoft Edge **Version:** 122.0.2365.59			
8528	C:\WINDOWS\system32\srtasks.exe ExecuteScopeRestorePoint /WaitForRestorePoint:11	C:\Windows\System32\SrTasks.exe	—	msiexec.exe
	Information **User:** SYSTEM **Company:** Microsoft Corporation **Integrity Level:** SYSTEM **Description:** Microsoft® Windows System Protection background tasks. **Exit code:** 0 **Version:** 10.0.19041.1 (WinBuild.160101.0800)			
8604	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	—	SrTasks.exe
	Information **User:** SYSTEM **Company:** Microsoft Corporation **Integrity Level:** SYSTEM **Description:** Console Window Host **Exit code:** 0 **Version:** 10.0.19041.1 (WinBuild.160101.0800)			
9136	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=39 --mojo-platform-channel-handle=5940 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
	Information **User:** admin **Company:** Microsoft Corporation **Integrity Level:** LOW **Description:** Microsoft Edge **Version:** 122.0.2365.59			
2420	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --extension-process --renderer-sub-type=extension --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=40 --mojo-platform-channel-handle=7868 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:2	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
	Information **User:** admin **Company:** Microsoft Corporation **Integrity Level:** LOW **Description:** Microsoft Edge **Exit code:** 0 **Version:** 122.0.2365.59			
8948	C:\Windows\syswow64\MsiExec.exe -Embedding 2D329B39EB43627C8473EFA0EA76E52E	C:\Windows\SysWOW64\msiexec.exe	☣ ⇆	msiexec.exe
	Information **User:** admin **Company:** Microsoft Corporation **Integrity Level:** MEDIUM **Description:** Windows® installer **Exit code:** 0 **Version:** 5.0.19041.3636 (WinBuild.160101.0800)			
2108	"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 --no-appcompat-clear --mojo-platform-channel-handle=6832 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
	Information **User:** admin **Company:** Microsoft Corporation **Integrity Level:** LOW **Description:** Microsoft Edge **Version:** 122.0.2365.59			

PID	CMD	Path	Indicators	Parent process
7872	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=8096 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

7744	C:\WINDOWS\System32\slui.exe -Embedding	C:\Windows\System32\slui.exe		svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Activation Client
Exit code:	0	Version:	10.0.19041.1 (WinBuild.160101.0800)

2332	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=8212 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

9076	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\onestart_installer.exe" "INSTALL" "15" "2" "1" "1"	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\onestart_installer.exe		msiexec.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	MEDIUM	Description:	OneStart Installer
Exit code:	0	Version:	132.0.6834.116

7740	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\setup.exe" --install-archive="C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\ONESTART.PACKED.7Z" "INSTALL" "15" "2" "1" "1"	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\setup.exe		onestart_installer.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	MEDIUM	Description:	OneStart Installer
Exit code:	0	Version:	132.0.6834.116

7932	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\setup.exe" --type=crashpad-handler /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Crashpad" --annotation=plat=Win64 --annotation=prod=OneStart --annotation=ver=132.0.6834.116 --initial-client-data=0x28c,0x290,0x294,0x268,0x298,0x7ff6d879e2f8,0x7ff6d879e304,0x7ff6d879e310	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\setup.exe	—	setup.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	MEDIUM	Description:	OneStart Installer
Exit code:	0	Version:	132.0.6834.116

780	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=8296 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

2392	"C:\Program Files\Google\Chrome\Application\122.0.6261.70\notification_helper.exe" -Embedding	C:\Program Files\Google\Chrome\Application\122.0.6261.70\notification_helper.exe		svchost.exe

PID	CMD	Path	Indicators	Parent process
	Information			
	User: admin **Company:** Google LLC			
	Integrity Level: MEDIUM **Description:** Google Chrome			
	Exit code: 0 **Version:** 122.0.6261.70			
4868	"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=122.0.6261.70 --initial-client-data=0x1f4,0x1f8,0x1fc,0x1d0,0x200,0x7ff6df3235f0,0x7ff6df3235fc,0x7ff6df323608	C:\Program Files\Google\Chrome\Application\chrome.exe	—	notification_helper.exe
	Information			
	User: admin **Company:** Google LLC			
	Integrity Level: MEDIUM **Description:** Google Chrome			
	Exit code: 0 **Version:** 122.0.6261.70			
8648	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\setup.exe" --verbose-logging --create-shortcuts=0 --install-level=0	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\setup.exe	—	setup.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: MEDIUM **Description:** OneStart Installer			
	Exit code: 73 **Version:** 132.0.6834.116			
8352	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\setup.exe" --type=crashpad-handler /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Crashpad" --annotation=plat=Win64 --annotation=prod=OneStart --annotation=ver=132.0.6834.116 --initial-client-data=0x29c,0x2a0,0x2a4,0x278,0x2a8,0x7ff6d879e2f8,0x7ff6d879e304,0x7ff6d879e310	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\setup.exe	—	setup.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: MEDIUM **Description:** OneStart Installer			
	Exit code: 0 **Version:** 132.0.6834.116			
1280	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --from-installer	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe		setup.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: MEDIUM **Description:** OneStart			
	Version: 132.0.6834.116			
7780	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Crashpad" --annotation=plat=Win64 --annotation=prod=OneStart --annotation=ver=132.0.6834.116 --initial-client-data=0x128,0x12c,0x130,0x104,0x134,0x7ffc88c4dcf8,0x7ffc88c4dd04,0x7ffc88c4dd10	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: MEDIUM **Description:** OneStart			
	Version: 132.0.6834.116			
1676	"C:\Windows\SysWOW64\cmd.exe" /c "rmdir /s /q "C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\""	C:\Windows\SysWOW64\cmd.exe	—	msiexec.exe
	Information			
	User: admin **Company:** Microsoft Corporation			
	Integrity Level: MEDIUM **Description:** Windows Command Processor			
	Exit code: 0 **Version:** 10.0.19041.3636 (WinBuild.160101.0800)			
1388	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	—	cmd.exe

PID	CMD	Path	Indicators	Parent process

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Console Window Host
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

7748	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=gpu-process --string-annotations --start-stack-profiler --gpu-preferences=UAAAAAAAAADgAAAEAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAAAAA --field-trial-handle=2036,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=2024 /prefetch:2	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	LOW	**Description:**	OneStart
Version:	132.0.6834.116		

4652	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --string-annotations --start-stack-profiler --field-trial-handle=2268,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=2308 /prefetch:3	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	↔	onestart.exe

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	MEDIUM	**Description:**	OneStart
Version:	132.0.6834.116		

3192	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=2464,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=2484 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	LOW	**Description:**	OneStart
Version:	132.0.6834.116		

3012	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --update	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	↔	onestart.exe

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	MEDIUM	**Description:**	OneStart
Exit code:	0	**Version:**	132.0.6834.116

7148	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --start-stack-profiler --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=6 --field-trial-handle=4016,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=4024 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	LOW	**Description:**	OneStart
Exit code:	0	**Version:**	132.0.6834.116

5972	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --field-trial-handle=4052,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=4168 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	LOW	**Description:**	OneStart

PID	CMD	Path	Indicators	Parent process
	Exit code: 0 **Version:** 132.0.6834.116			
900	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe" --type=renderer --string-annotations --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=7 --field-trial-handle=4980,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5032 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: LOW **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			
9132	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe" --type=renderer --string-annotations --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=8 --field-trial-handle=5052,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5116 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: LOW **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			
4932	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=4968,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5284 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: LOW **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			
8776	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5284,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5444 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: LOW **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			
7736	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe" --type=utility --utility-sub-type=chrome.mojom.ProcessorMetrics --lang=en-US --service-sandbox-type=none --string-annotations --field-trial-handle=5848,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5884 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: MEDIUM **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			
7596	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5924,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5952 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: LOW **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			

PID	CMD	Path	Indicators	Parent process
8632	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5936,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5928 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
Information				
User: admin	**Company:** OneStart.ai			
Integrity Level: LOW	**Description:** OneStart			
Exit code: 0	**Version:** 132.0.6834.116			
8436	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=6088,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5884 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
Information				
User: admin	**Company:** OneStart.ai			
Integrity Level: LOW	**Description:** OneStart			
Exit code: 0	**Version:** 132.0.6834.116			
8360	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5304,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=6124 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
Information				
User: admin	**Company:** OneStart.ai			
Integrity Level: LOW	**Description:** OneStart			
Exit code: 0	**Version:** 132.0.6834.116			
8912	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5328,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=6216 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
Information				
User: admin	**Company:** OneStart.ai			
Integrity Level: LOW	**Description:** OneStart			
Exit code: 0	**Version:** 132.0.6834.116			
4300	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5408,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=6336 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
Information				
User: admin	**Company:** OneStart.ai			
Integrity Level: LOW	**Description:** OneStart			
Exit code: 0	**Version:** 132.0.6834.116			
6512	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=6208,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=6204 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
Information				
User: admin	**Company:** OneStart.ai			
Integrity Level: LOW	**Description:** OneStart			
Exit code: 0	**Version:** 132.0.6834.116			
5984	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=6212,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5260 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

PID	CMD	Path	Indicators	Parent process

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	LOW	Description:	OneStart
Exit code:	0	Version:	132.0.6834.116

8712	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --extension-process --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=20 --field-trial-handle=6008,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=6484 /prefetch:2	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	LOW	Description:	OneStart
Exit code:	0	Version:	132.0.6834.116

8668	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5996,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=6016 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe		onestart.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	LOW	Description:	OneStart
Exit code:	0	Version:	132.0.6834.116

2152	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=8236 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	122.0.2365.59

9008	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5844,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=4252 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	LOW	Description:	OneStart
Exit code:	0	Version:	132.0.6834.116

856	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5040,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=3896 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	LOW	Description:	OneStart
Exit code:	0	Version:	132.0.6834.116

8868	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=4252,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=3164 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	LOW	Description:	OneStart

PID	CMD	Path	Indicators	Parent process
	Exit code: 0 **Version:** 132.0.6834.116			
1532	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=3052,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=4248 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: LOW **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			
1852	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=4024,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=4280 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: LOW **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			
6724	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=6472,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=3432 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: LOW **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			
5500	"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=10.0.19041.3636 --no-appcompat-clear --gpu-preferences=WAAAAAAAAADoAAAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAABEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=1980 --field-trial-handle=2324,i,1502768736322576 05,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
	Information			
	User: admin **Company:** Microsoft Corporation			
	Integrity Level: MEDIUM **Description:** Microsoft Edge			
	Exit code: 0 **Version:** 122.0.2365.59			
8696	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe"	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	explorer.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: MEDIUM **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			
8472	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data" /prefetch:4 --monitor-self --monitor-self-argument=--type=crashpad-handler "--monitor-self-argument=--user-data-dir=C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data" --monitor-self-argument=/prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin \AppData\Local\OneStart.ai\OneStart\User Data\Crashpad" --annotation=plat=Win64 --annotation=prod=OneStart --annotation=ver=132.0.6834.116 --initial-client-data=0x148,0x14c,0x150,0x124,0x154,0x7ffc88c4dcf8,0x7ffc88c4dd04,0x7ffc88c4dd10	C:\Users\admin\AppData\Local\OneStart.ai\OneStart \Application\onestart.exe	—	onestart.exe
	Information			
	User: admin **Company:** OneStart.ai			
	Integrity Level: MEDIUM **Description:** OneStart			
	Exit code: 0 **Version:** 132.0.6834.116			

PID	CMD	Path	Indicators	Parent process
8080	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data" /prefetch:4 --no-periodic-tasks --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Crashpad" --annotation=plat=Win64 --annotation=prod=OneStart --annotation=ver=132.0.6834.116 --initial-client-data=0x1b4,0x1b8,0x1bc,0x174,0x1c0,0x7ff79e1e3840,0x7ff79e1e384c,0x7ff79e1e3858	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
1600	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --start-stack-profiler --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=29 --field-trial-handle=4376,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=2516 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
5380	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=28 --field-trial-handle=4404,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=4100 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
3396	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --extension-process --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=30 --field-trial-handle=4348,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=4140 /prefetch:2	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
4464	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=31 --field-trial-handle=6776,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=6140 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
540	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=32 --field-trial-handle=2496,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5140 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	MEDIUM	**Description:**	OneStart
Exit code:	0	**Version:**	132.0.6834.116

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	LOW	**Description:**	OneStart
Exit code:	0	**Version:**	132.0.6834.116

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	LOW	**Description:**	OneStart
Exit code:	0	**Version:**	132.0.6834.116

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	LOW	**Description:**	OneStart
Exit code:	0	**Version:**	132.0.6834.116

Information

User:	admin	**Company:**	OneStart.ai
Integrity Level:	LOW	**Description:**	OneStart
Exit code:	0	**Version:**	132.0.6834.116

Information

User:	admin	**Company:**	OneStart.ai

PID	CMD	Path	Indicators	Parent process
	Integrity Level: LOW **Description:** OneStart **Exit code:** 0 **Version:** 132.0.6834.116			
5740	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=7656 --field-trial-handle=2324,i,150276873632257605,5236874692018770281,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe
	Information **User:** admin **Company:** Microsoft Corporation **Integrity Level:** LOW **Description:** Microsoft Edge **Exit code:** 0 **Version:** 122.0.2365.59			
896	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=33 --field-trial-handle=7056,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=6952 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
	Information **User:** admin **Company:** OneStart.ai **Integrity Level:** LOW **Description:** OneStart **Exit code:** 0 **Version:** 132.0.6834.116			
8748	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=renderer --string-annotations --start-stack-profiler --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=34 --field-trial-handle=4284,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5076 /prefetch:1	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
	Information **User:** admin **Company:** OneStart.ai **Integrity Level:** LOW **Description:** OneStart **Exit code:** 0 **Version:** 132.0.6834.116			
7932	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=4556,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=4464 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
	Information **User:** admin **Company:** OneStart.ai **Integrity Level:** LOW **Description:** OneStart **Exit code:** 0 **Version:** 132.0.6834.116			
6392	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=5320,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=3800 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
	Information **User:** admin **Company:** OneStart.ai **Integrity Level:** LOW **Description:** OneStart **Exit code:** 0 **Version:** 132.0.6834.116			
9096	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=2924,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=5928 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe
	Information **User:** admin **Company:** OneStart.ai **Integrity Level:** LOW **Description:** OneStart **Exit code:** 0 **Version:** 132.0.6834.116			

PID	CMD	Path	Indicators	Parent process
8372	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=4944,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=3692 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	LOW	Description:	OneStart
Exit code:	0	Version:	132.0.6834.116

8352	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=6808,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=3836 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	LOW	Description:	OneStart
Exit code:	0	Version:	132.0.6834.116

7940	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --string-annotations --field-trial-handle=4448,i,8289675821031646596,7972186531293721172,262144 --variations-seed-version --mojo-platform-channel-handle=4608 /prefetch:8	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	—	onestart.exe

Information

User:	admin	Company:	OneStart.ai
Integrity Level:	LOW	Description:	OneStart
Exit code:	0	Version:	132.0.6834.116

6736	"C:\WINDOWS\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe	—	svchost.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	Windows Shell Experience Host
Version:	10.0.19041.3758 (WinBuild.160101.0800)		

Registry activity

Total events	Read events	Write events	Delete events
29 764	29 348	394	22

Modification events

(PID) Process:	(3956) msedge.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation:	write	Name:	failed_count
Value:	0		

(PID) Process:	(3956) msedge.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation:	write	Name:	state
Value:	2		

(PID) Process:	(3956) msedge.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation:	write	Name:	state
Value:	1		

(PID) Process:	(3956) msedge.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\StabilityMetrics
Operation:	write	Name:	user_experience_metrics.stability.exited_cleanly
Value:	0		

(PID) Process:	(3956) msedge.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\ClientStateMedium\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}\LastWasDefault
Operation:	write	Name:	S-1-5-21-1693682860-607145093-2874071422-1001

Value: 446F8DB7508E2F00

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {35BD4AD9-A655-45A3-884A-254E1ECCF3B0}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {1CDB5ADA-48A1-4EE4-8C9C-1F7A69429C54}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {82518951-4362-44F2-8C0B-1B46C1588C47}

(PID) Process: (3956) msedge.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\ClientStateMedium\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}\LastWasDefault
Operation: write **Name:** S-1-5-21-1693682860-607145093-2874071422-1001
Value: AAD198B7508E2F00

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {B45268EA-09C7-40E7-B249-4DD5FDA4DBAB}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {299A8DCC-9A45-44A6-94F6-8B5A16D2D23B}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {941F258C-2A6B-4AD8-8C83-AB2FCC1EA2DE}

(PID) Process: (3956) msedge.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\ClientStateMedium\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}\LastWasDefault
Operation: write **Name:** S-1-5-21-1693682860-607145093-2874071422-1001
Value: 464DF8B7508E2F00

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation: write **Name:** MicrosoftEdgeAutoLaunch_29EBC4579851B72EE312C449CF839B1A
Value: "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\EdgeUpdate\Clients\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}\Commands\on-logon-autolaunch
Operation: write **Name:** Enabled
Value: 0

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\Profiles
Operation: write **Name:** EnhancedLinkOpeningDefault
Value: Default

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {FA66B27F-442E-4923-8A7D-E641D4971D2A}

(PID) Process: (8452) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached
Operation: write **Name:** {2781761E-28E0-4109-99FE-B9D127C57AFE} {56FFCC30-D398-11D0-B2AE-00A0C908FA49} 0xFFFF
Value: 010000000000000091CDD830278FDB01

(PID) Process: (8732) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (8732) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (8732) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (9004) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (9004) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies

Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (9004) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.msi\OpenWithProgids
Operation: write **Name:** Msi.Package
Value:

(PID) Process: (9200) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (9200) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (9200) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (8544) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (8544) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (8544) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (8264) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (8264) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (8264) BackgroundTransferHost.exe **Key:** HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Storage\microsoft.windows.contentdeliverymanager_cw5n1h2txyewy\Internet Settings\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SystemRestore
Operation: write **Name:** SrCreateRp (Enter)
Value: 4800000000000005DF3173F278FDB01942200005C230000D5070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGetSnapshots (Enter)
Value: 4800000000000000BD41183F278FDB01942200005C230000D2070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppEnumGroups (Leave)
Value: 4800000000000000006C613F278FDB01942200005C230000D1070000010000000000000001000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SPP
Operation: write **Name:** LastIndex
Value: 11

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGetSnapshots (Leave)
Value: 4800000000000001E095F3F278FDB01942200005C230000D2070000010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppEnumGroups (Enter)

Value: 4800000000000000031D5F3F278FDB01942200005C230000D1070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppCreate (Enter)
Value: 4800000000000000A377643F278FDB01942200005C230000D0070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGatherWriterMetadata (Enter)
Value: 4800000000000000F7AED93F278FDB01942200005C230000D3070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
Operation: write **Name:** IDENTIFY (Enter)
Value: 4800000000000000007C9ADC3F278FDB01942200007C060000E8030000010000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** IDENTIFY (Leave)
Value: 4800000000000000B47DEE3F278FDB01642300002423000E8030000000000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** IDENTIFY (Leave)
Value: 4800000000000000FFC3F13F278FDB0164230000CC0B0000E8030000000000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\ASR Writer
Operation: write **Name:** IDENTIFY (Leave)
Value: 4800000000000000096FEF23F278FDB01642300002023000E8030000000000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** IDENTIFY (Enter)
Value: 4800000000000000AD1DE83F278FDB0164230000CC0B0000E8030000010000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** IDENTIFY (Enter)
Value: 4800000000000000AD1DE83F278FDB01642300001C230000E8030000010000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\ASR Writer
Operation: write **Name:** IDENTIFY (Enter)
Value: 4800000000000000006C40E93F278FDB01642300002023000E8030000010000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** IDENTIFY (Enter)
Value: 4800000000000000006C40E93F278FDB01642300002423000E8030000010000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** IDENTIFY (Leave)
Value: 4800000000000000004555ED3F278FDB01642300001C230000E8030000000000000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{9dea862c-5cdd-4e70-acc1-f32b344d4795}\Elements\11000001
Operation: delete key **Name:** (default)
Value:

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{9dea862c-5cdd-4e70-acc1-f32b344d4795}\Elements\11000001
Operation: write **Name:** Element
Value: 0000000000000000000000000000000000060000000000000048000000000000000715E5C2FA985EB1190A89A9B763584210000000000000000745E5C2FA985EB1190A89A9B763584210000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{9dea862c-5cdd-4e70-acc1-f32b344d4795}\Elements\12000002
Operation: delete key **Name:** (default)
Value:

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{9dea862c-5cdd-4e70-acc1-f32b344d4795}\Elements\12000002
Operation: write **Name:** Element
Value: \EFI\Microsoft\Boot\bootmgfw.efi

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{5b970157-8568-11eb-b45c-806e6f6e6963}\Elements\11000001
Operation: delete key **Name:** (default)
Value:

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{5b970157-8568-11eb-b45c-806e6f6e6963}\Elements\11000001
Operation: write **Name:** Element
Value: 0000000000000000000000000000000000060000000000000048000000000000000715E5C2FA985EB1190A89A9B763584210000000000000000745E5C2FA985EB1190A89A9B763584210000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{5b970157-8568-11eb-b45c-806e6f6e6963}\Elements\12000002
Operation: delete key **Name:** (default)
Value:

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{5b970157-8568-11eb-b45c-806e6f6e6963}\Elements\12000002

Operation: write **Name:** Element
Value: \EFI\Boot\Loader.efi

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{a5a30fa2-3d06-4e9f-b5f4-a01df9d1fcba}\Description
Operation: delete key **Name:** (default)
Value:

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{a5a30fa2-3d06-4e9f-b5f4-a01df9d1fcba}\Elements\24000001
Operation: delete key **Name:** (default)
Value:

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{a5a30fa2-3d06-4e9f-b5f4-a01df9d1fcba}\Elements\25000004
Operation: delete key **Name:** (default)
Value:

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{a5a30fa2-3d06-4e9f-b5f4-a01df9d1fcba}\Elements
Operation: delete key **Name:** (default)
Value:

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{a5a30fa2-3d06-4e9f-b5f4-a01df9d1fcba}
Operation: delete key **Name:** (default)
Value:

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{a5a30fa2-3d06-4e9f-b5f4-a01df9d1fcba}\Description
Operation: write **Name:** Type
Value: 269484033

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{a5a30fa2-3d06-4e9f-b5f4-a01df9d1fcba}\Elements\24000001
Operation: write **Name:** Element
Value: {5b970157-8568-11eb-b45c-806e6f6e6963}

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\BCD00000000\Objects\{a5a30fa2-3d06-4e9f-b5f4-a01df9d1fcba}\Elements\25000004
Operation: write **Name:** Element
Value: 0000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
Operation: write **Name:** IDENTIFY (Leave)
Value: 480000000000000001F63542278FDB01942200007C060000E8030000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {8DC78323-1200-4C0F-BAF0-E69814D45CF8}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {45AA8F84-6545-4080-94DA-B37B5AE7251D}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {01F4A382-B86F-474F-9648-A1D3027B9613}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {008A6A06-1BF9-43DA-AC65-C0AAA8DC71C2}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {9824F0AF-50ED-4223-9445-31F485E31030}

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGatherWriterMetadata (Leave)
Value: 480000000000000022A15E46278FDB01942200005C230000D3070000010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppAddInterestingComponents (Enter)
Value: 480000000000000022A15E46278FDB01942200005C230000D4070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {52ED80CF-9937-46C9-8B46-ECA0B828CBB5}

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppAddInterestingComponents (Leave)
Value: 480000000000000009E76A746278FDB01942200005C230000D4070000010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}

Operation: write **Name:** PROVIDER_BEGINPREPARE (Enter)
Value: 4800000000000000E3EBDE46278FDB0164230000202300000104000001000000000000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_BEGINPREPARE (Leave)
Value: 4800000000000000BD75E046278FDB0164230000202300000104000000000000000000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
Operation: write **Name:** PREPAREBACKUP (Enter)
Value: 4800000000000000004275E146278FDB01942200008C200000E9030000010000000000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** PREPAREBACKUP (Enter)
Value: 4800000000000000E8D6E246278FDB0164230000202300000E9030000010000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** PREPAREBACKUP (Enter)
Value: 4800000000000000EFFEE246278FDB0164230000CC0B0000E9030000010000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** PREPAREBACKUP (Enter)
Value: 4800000000000000EFFEE246278FDB0164230000242300000E9030000010000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {8B673834-E7D4-4309-A6C1-1614B1A5B4FD}

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** PREPAREBACKUP (Leave)
Value: 4800000000000000DCD1EA46278FDB0164230000CC0B0000E9030000000000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** VSS_WS_STABLE (SetCurrentState)
Value: 4800000000000000002A9AEB46278FDB0164230000CC0B0000010000000010000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** PREPAREBACKUP (Leave)
Value: 4800000000000000C0F7EC46278FDB0164230000242300000E9030000000000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** VSS_WS_STABLE (SetCurrentState)
Value: 4800000000000000C0F7EC46278FDB0164230000242300000100000001000000010000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** PREPAREBACKUP (Leave)
Value: 4800000000000000300BEE46278FDB0164230000202300000E9030000000000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** VSS_WS_STABLE (SetCurrentState)
Value: 4800000000000000300BEE46278FDB0164230000202300000100000001000000010000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
Operation: write **Name:** PREPAREBACKUP (Leave)
Value: 4800000000000000008D1B3147278FDB01942200008C200000E9030000000000000000000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** GETSTATE (Leave)
Value: 4800000000000000E6C14147278FDB0164230000242300000F9030000000000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** GETSTATE (Leave)
Value: 4800000000000000E6C14147278FDB0164230000202300000F9030000000000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** GETSTATE (Leave)
Value: 4800000000000000343B4247278FDB0164230000CC0B0000F9030000000000000100000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {8F675C2C-4CBC-4513-8C21-B3182B20CDC4}

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
Operation: write **Name:** GETSTATE (Enter)
Value: 4800000000000000C1B33647278FDB0194220000CC200000F9030000010000000000000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer

Operation: write **Name:** GETSTATE (Enter)
Value: 4800000000000000051583F47278FDB0164230000242300 00F9030000010000000100000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** GETSTATE (Enter)
Value: 4800000000000000051583F47278FDB0164230000202300 00F9030000010000000100000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** GETSTATE (Enter)
Value: 4800000000000000D0F4147278FDB0164230000CC0B0000F9030000010000000100000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
Operation: write **Name:** GETSTATE (Leave)
Value: 4800000000000000003634347278FDB0194220000CC200000F9030000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
Operation: write **Name:** DOSNAPSHOT (Enter)
Value: 4800000000000000C34C8C47278FDB01942200005C2300000A0400000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_ENDPREPARE (Enter)
Value: 4800000000000000E9F58D47278FDB0164230000AC2000000204000001000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {50AC2907-E89F-4200-AA33-7EE44739B5D9}

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** PREPARESNAPSHOT (Enter)
Value: 4800000000000000872FEF47278FDB0164230000442000 00EA0300000100000001000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** PREPARESNAPSHOT (Leave)
Value: 4800000000000000 4E17FD47278FDB0164230000802000 00EA0300000000000001000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_FREEZE (SetCurrentState)
Value: 4800000000000000 4E17FD47278FDB0164230000802000000200000001000000010000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** PREPARESNAPSHOT (Leave)
Value: 4800000000000000 18550848278FDB0164230000402000 00EA0300000000000001000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_FREEZE (SetCurrentState)
Value: 4800000000000000 18550848278FDB0164230000402000000200000001000000010000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** PREPARESNAPSHOT (Leave)
Value: 4800000000000000033A40848278FDB0164230000442000 00EA0300000000000001000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_FREEZE (SetCurrentState)
Value: 4800000000000000033A40848278FDB0164230000442000000200000001000000010000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_ENDPREPARE (Leave)
Value: 4800000000000000 5ACBE547278FDB0164230000AC2000000204000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** PREPARESNAPSHOT (Enter)
Value: 4800000000000000 4536EC47278FDB0164230000AC200000EA0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** PREPARESNAPSHOT (Enter)
Value: 4800000000000000FAF3ED47278FDB0164230000802000 00EA0300000100000001000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** PREPARESNAPSHOT (Enter)
Value: 4800000000000000 9491EE47278FDB0164230000402000 00EA0300000100000001000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** PREPARESNAPSHOT (Leave)
Value: 4800000000000000B6B75248278FDB0164230000AC200000EA0300000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher

Operation: write **Name:** FREEZE (Enter)
Value: 4800000000000000B6B75248278FDB0164230000AC200000EB0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_FRONT (Enter)
Value: 4800000000000000B6B75248278FDB0164230000AC200000EC0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** FREEZE (Enter)
Value: 4800000000000000B6B75248278FDB0164230000482000 0EB0300000100000002000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** FREEZE (Leave)
Value: 4800000000000000B6B75248278FDB0164230000482000 00EB0300000000000002000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_THAW (SetCurrentState)
Value: 4800000000000000B6B75248278FDB0164230000482000003000000100000002000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** BKGND_FREEZE_THREAD (Enter)
Value: 4800000000000000B6B75248278FDB0164230000DC210000FC0300000100000003000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_FRONT (Leave)
Value: 4800000000000000DE1A5548278FDB0164230000AC200000EC0300000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_BACK (Enter)
Value: 4800000000000000DE1A5548278FDB0164230000AC200000ED0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_BACK (Leave)
Value: 4800000000000000DE1A5548278FDB0164230000AC200000ED0300000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_SYSTEM (Enter)
Value: 4800000000000000DE1A5548278FDB0164230000AC200000EE0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** FREEZE (Enter)
Value: 4800000000000000 5E855748278FDB0164230000C200000EB0300000100000002000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** FREEZE (Leave)
Value: 4800000000000000 5E855748278FDB0164230000C200000EB0300000000000002000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_THAW (SetCurrentState)
Value: 4800000000000000 5E855748278FDB0164230000C2000000300000001000000020000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** BKGND_FREEZE_THREAD (Enter)
Value: 4800000000000000 5E855748278FDB0164230003C220000FC0300000100000003000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_SYSTEM (Leave)
Value: 4800000000000000 8A3F5C48278FDB0164230000AC200000EE0300000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_KTM (Enter)
Value: 4800000000000000 8A3F5C48278FDB0164230000AC200000F0030000010000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_KTM (Leave)
Value: 4800000000000000 8A3F5C48278FDB0164230000AC200000F0030000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_RM (Enter)
Value: 4800000000000000 8A3F5C48278FDB0164230000AC200000EF0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** FREEZE (Enter)
Value: 4800000000000000 8A3F5C48278FDB0164230000 40200000EB0300000100000002000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer

Operation: write **Name:** FREEZE (Leave)
Value: 4800000000000000034222E49278FDB0164230000040200000EB0300000000000002000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_THAW (SetCurrentState)
Value: 4800000000000000034222E49278FDB0164230000040200000030000000100000002000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE_RM (Leave)
Value: 4800000000000000034222E49278FDB0164230000AC200000EF0300000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** FREEZE (Leave)
Value: 4800000000000000034222E49278FDB0164230000AC200000EB0300000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** BKGND_FREEZE_THREAD (Enter)
Value: 4800000000000000034222E49278FDB0164230000B4210000FC0300000100000003000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_PRECOMMIT (Enter)
Value: 4800000000000000034222E49278FDB0164230000AC2000000304000001000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_PRECOMMIT (Leave)
Value: 4800000000000000034222E49278FDB0164230000AC2000000304000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace
Operation: write **Name:** OPEN_VOLUME_HANDLE (Enter)
Value: 4800000000000000034222E49278FDB0164230000AC200000FD0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(__?_Volume{2f5c5e72-85a9-11eb-90a8-9a9b76358421}_)
Operation: write **Name:** OPEN_VOLUME_HANDLE (Enter)
Value: 4800000000000000034222E49278FDB0164230000B8210000FD0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(__?_Volume{2f5c5e72-85a9-11eb-90a8-9a9b76358421}_)
Operation: write **Name:** OPEN_VOLUME_HANDLE (Leave)
Value: 4800000000000000002056E049278FDB0164230000B8210000FD0300000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace
Operation: write **Name:** OPEN_VOLUME_HANDLE (Leave)
Value: 4800000000000000002056E049278FDB0164230000AC200000FD0300000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_POSTCOMMIT (Leave)
Value: 4800000000000000093E80C4A278FDB0164230000AC2000000504000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** THAW_KTM (Enter)
Value: 4800000000000000000100D4A278FDB0164230000AC200000F4030000010000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** THAW_KTM (Leave)
Value: 4800000000000000000100D4A278FDB0164230000AC200000F4030000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** THAW (Enter)
Value: 4800000000000000000100D4A278FDB0164230000AC200000F2030000010000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** THAW (Enter)
Value: 4800000000000000AA720D4A278FDB0164230000402000000F2030000010000000300000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** BKGND_FREEZE_THREAD (Leave)
Value: 4800000000000000AA720D4A278FDB0164230000DC210000FC0300000000000003000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** THAW (Enter)
Value: 4800000000000000AA720D4A278FDB0164230000482000000F2030000010000000300000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** BKGND_FREEZE_THREAD (Leave)
Value: 4800000000000000AA720D4A278FDB0164230000003C220000FC0300000000000003000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** THAW (Leave)
Value: 4800000000000000AA720D4A278FDB0164230000402000 0F2030000000000000300000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_POST_SNAPSHOT (SetCurrentState)
Value: 4800000000000000AA720D4A278FDB0164230000402000000400000001000000030000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** THAW (Leave)
Value: 4800000000000000AA720D4A278FDB0164230000482000 0F2030000000000000300000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_POST_SNAPSHOT (SetCurrentState)
Value: 4800000000000000AA720D4A278FDB0164230000482000000400000001000000030000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** THAW (Enter)
Value: 4800000000000000929A0D4A278FDB01642300000C200000F2030000010000000300000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** BKGND_FREEZE_THREAD (Leave)
Value: 4800000000000000929A0D4A278FDB0164230000B4210000FC0300000000000000300000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** THAW (Leave)
Value: 4800000000000000929A0D4A278FDB01642300000C200000F2030000000000000300000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_POST_SNAPSHOT (SetCurrentState)
Value: 4800000000000000929A0D4A278FDB01642300000C2000000400000001000000030000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** THAW (Leave)
Value: 4800000000000000BC20D4A278FDB0164230000AC200000F2030000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_PREFINALCOMMIT (Enter)
Value: 4800000000000000BC20D4A278FDB0164230000AC2000000604000001000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(__?_Volume{2f5c5e72-85a9-11eb-90a8-9a9b76358421}_)
Operation: write **Name:** IOCTL_FLUSH_AND_HOLD (Enter)
Value: 4800000000000002056E049278FDB0164230000B8210000FE0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(__?_Volume{2f5c5e72-85a9-11eb-90a8-9a9b76358421}_)
Operation: write **Name:** IOCTL_FLUSH_AND_HOLD (Leave)
Value: 4800000000000006B5C0A4A278FDB0164230000B8210000FE0300000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(__?_Volume{2f5c5e72-85a9-11eb-90a8-9a9b76358421}_)
Operation: write **Name:** IOCTL_RELEASE (Enter)
Value: 4800000000000006B5C0A4A278FDB0164230000B8210000FF0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace(__?_Volume{2f5c5e72-85a9-11eb-90a8-9a9b76358421}_)
Operation: write **Name:** IOCTL_RELEASE (Leave)
Value: 4800000000000006B5C0A4A278FDB0164230000B8210000FF0300000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace
Operation: write **Name:** IOCTL_FLUSH_AND_HOLD (Enter)
Value: 4800000000000002056E049278FDB0164230000AC200000FE0300000100000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace
Operation: write **Name:** IOCTL_FLUSH_AND_HOLD (Leave)
Value: 4800000000000006B5C0A4A278FDB0164230000AC200000FE0300000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace
Operation: write **Name:** IOCTL_RELEASE (Enter)
Value: 4800000000000006B5C0A4A278FDB0164230000AC200000FF0300000100000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Lovelace
Operation: write **Name:** IOCTL_RELEASE (Leave)
Value: 4800000000000006B5C0A4A278FDB0164230000AC200000FF0300000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}

Operation: write **Name:** PROVIDER_COMMIT (Enter)
Value: 48000000000000006B5C0A4A278FDB0164230000AC210000040400000100000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_COMMIT (Leave)
Value: 48000000000000006B5C0A4A278FDB0164230000AC210000040400000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_POSTCOMMIT (Enter)
Value: 48000000000000000D1830A4A278FDB0164230000AC200000050400000100000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssapiPublisher
Operation: write **Name:** DOSNAPSHOT (Leave)
Value: 48000000000000000100D4A278FDB0194220000A02000000A0400000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppCreate (Leave)
Value: 480000000000000893E0E4A278FDB01942200005C230000D0070000010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SystemRestore
Operation: write **Name:** SrCreateRp (Leave)
Value: 480000000000000893E0E4A278FDB01942200005C230000D5070000010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore
Operation: write **Name:** FirstRun
Value: 0

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore
Operation: write **Name:** LastIndex
Value: 11

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\Volatile
Operation: write **Name:** NestingLevel
Value: 1

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\Volatile
Operation: write **Name:** StartNesting
Value: 93A4173F278FDB01

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {D1B057CE-8162-4DC5-A9DE-FA4E0D86896D}

(PID) Process: (8852) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation: write **Name:** Owner
Value: 94220000E9A40535278FDB01

(PID) Process: (8852) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation: write **Name:** SessionHash
Value: 0FBE67603B786C8DBF662309801CB5A1772E31315FF4CBB63EA31EFDCF7A2DB9

(PID) Process: (8852) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation: write **Name:** Sequence
Value: 1

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {9BCFE363-EAEA-4F49-81A5-9A68AA3AE83B}

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGetSnapshots (Enter)
Value: 4800000000000000E79FBE4A278FDB01502100006C210000D2070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_PREFINALCOMMIT (Leave)
Value: 48000000000000005A3ADF4A278FDB0164230000AC200000060400000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppEnumGroups (Leave)
Value: 48000000000000001A7FFF4A278FDB01502100006C210000D1070000010000000000000001000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** POSTSNAPSHOT (Enter)
Value: 48000000000000003B76EC4A278FDB0164230000AC200000F5030000010000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer

Operation: write **Name:** POSTSNAPSHOT (Enter)
Value: 48000000000000003B76EC4A278FDB01642300008020000F503000001000000040000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** POSTSNAPSHOT (Enter)
Value: 48000000000000003B76EC4A278FDB01642300004420000F503000001000000040000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** POSTSNAPSHOT (Enter)
Value: 48000000000000003B76EC4A278FDB01642300004020000F503000001000000040000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** POSTSNAPSHOT (Leave)
Value: 48000000000000056DAEE4A278FDB01642300004420000F503000000000000040000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_BACKUP_COMPLETE (SetCurrentState)
Value: 48000000000000056DAEE4A278FDB01642300004420000005000000010000000400000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** POSTSNAPSHOT (Leave)
Value: 48000000000000056DAEE4A278FDB01642300004020000F503000000000000040000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_BACKUP_COMPLETE (SetCurrentState)
Value: 48000000000000056DAEE4A278FDB01642300004020000005000000010000000400000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGetSnapshots (Leave)
Value: 4800000000000000F6B7FA4A278FDB01502100006C210000D2070000010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppEnumGroups (Enter)
Value: 4800000000000000F6B7FA4A278FDB01502100006C210000D1070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_POSTFINALCOMMIT (Leave)
Value: 4800000000000000CFAB954B278FDB0164230000AC2000000704000000000000000000000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** BACKUPSHUTDOWN (Enter)
Value: 4800000000000000D1B4974B278FDB0164230000AC200000FB030000010000000000000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** BACKUPSHUTDOWN (Enter)
Value: 48000000000000002F72984B278FDB01642300004820000FB030000010000000500000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\COM+ REGDB Writer
Operation: write **Name:** BACKUPSHUTDOWN (Leave)
Value: 48000000000000002F72984B278FDB01642300004820000FB030000000000000500000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** BACKUPSHUTDOWN (Enter)
Value: 48000000000000002F72984B278FDB01642300008020000FB030000010000000500000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** BACKUPSHUTDOWN (Leave)
Value: 48000000000000002F72984B278FDB01642300008020000FB030000000000000500000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** BACKUPSHUTDOWN (Enter)
Value: 4800000000000000F699984B278FDB01642300004420000FB030000010000000500000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Registry Writer
Operation: write **Name:** BACKUPSHUTDOWN (Leave)
Value: 4800000000000000F699984B278FDB01642300004420000FB030000000000000500000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** BACKUPSHUTDOWN (Leave)
Value: 4800000000000000F699984B278FDB0164230000AC200000FB030000000000000000000000000000060F9433EB10A1644BF3AB0FB614D935000000000000000000000000000000000

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
Operation: write **Name:** C:\Config.Msi\
Value:

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Rollback\Scripts

Operation: write **Name:** C:\Config.Msi\117aac.rbs
Value: 31166247

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Rollback\Scripts
Operation: write **Name:** C:\Config.Msi\117aac.rbsLow
Value:

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
Operation: write **Name:** C:\Users\admin\AppData\Roaming\Microsoft\Installer\
Value:

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-21-1693682860-607145093-2874071422-1001\Components\A03F7ADAA09D97B41B78E25389937A65
Operation: write **Name:** 6D42462E5AA5C914BB9AB631827F0AB0
Value: C:\Users\admin\AppData\Local\OneStart.ai\

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-21-1693682860-607145093-2874071422-1001\Components\61A5E60DB477C9143876E54933DEE7F5
Operation: write **Name:** 6D42462E5AA5C914BB9AB631827F0AB0
Value: C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
Operation: write **Name:** C:\Users\admin\AppData\Local\OneStart.ai\
Value: 1

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
Operation: write **Name:** C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\
Value: 1

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** POSTSNAPSHOT (Leave)
Value: 480000000000000050C96E4B278FDB01642300008020000F5030000000000000400000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\Shadow Copy Optimization Writer
Operation: write **Name:** VSS_WS_WAITING_FOR_BACKUP_COMPLETE (SetCurrentState)
Value: 480000000000000050C96E4B278FDB01642300008020000005000000010000000400000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\VssvcPublisher
Operation: write **Name:** POSTSNAPSHOT (Leave)
Value: 480000000000000050C96E4B278FDB0164230000AC200000F5030000000000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (9060) VSSVC.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SwProvider_{b5946137-7b9f-4925-af80-51abd60b20d5}
Operation: write **Name:** PROVIDER_POSTFINALCOMMIT (Enter)
Value: 480000000000000050C96E4B278FDB0164230000AC200000070400000100000000000000000000000060F9433EB10A1644BF3AB0FB614D9350000000000000000000000000000000000

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {084F6767-CBC9-4204-A2E6-63C4CE51BF26}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {BD6BBDFD-314B-4874-9ECD-A53DB41CAB7A}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {FF2261A4-BE62-4BF3-9797-3CC57AC83F3F}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {62F638E2-AF57-4BD1-A7D2-3ACAFD2400D1}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {4041485B-5CED-4D8D-9D6B-8E92109F3808}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {68CC7B09-3D20-4BC7-A59F-748549120B0D}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {4AE0C0A1-8D1C-438A-A18F-BC466B0C8F56}

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGetSnapshots (Enter)
Value: 4800000000000000E21F2E51278FDB01502100006C210000D2070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGetSnapshots (Leave)
Value: 480000000000000091E02E51278FDB01502100006C210000D2070000010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppEnumGroups (Enter)
Value: 4800000000000000DB072F51278FDB01502100006C210000D1070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppEnumGroups (Leave)
Value: 480000000000000962F2F51278FDB01502100006C210000D1070000010000000000000010000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGetSnapshots (Enter)
Value: 4800000000000000CDF33251278FDB01502100006C210000D2070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppGetSnapshots (Leave)
Value: 48000000000000007BA53351278FDB01502100006C210000D2070000010000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppEnumGroups (Enter)
Value: 48000000000000007BA53351278FDB01502100006C210000D1070000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (8528) SrTasks.exe **Key:** HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\VSS\Diag\SPP
Operation: write **Name:** SppEnumGroups (Leave)
Value: 4800000000000000F7F33351278FDB01502100006C210000D1070000010000000000000010000000000000000000000000000000000000000000000000000000000000000000000000000000

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {69AB10C6-24AE-4651-BA17-8C6935066A41}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {9D575B73-43DD-4BAE-9481-49FC662DE46E}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {9956EE09-7D96-4FCA-829B-0D0DEC9DEE3F}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {C54C8A23-9C08-426C-AF92-086E4BCB14B0}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {E954F510-394C-4CC2-AF7B-8F83599D89C7}

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {690C9844-84B4-4F93-A58B-BA3577BCEFF6}

(PID) Process: (8852) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001_Classes\Local Settings\MuiCache\3c\52C64B7E
Operation: delete key **Name:** (default)
Value:

(PID) Process: (8852) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001_Classes\Local Settings\MuiCache\3c
Operation: delete key **Name:** (default)
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** InstallerProgress
Value: 25

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {D0DFD570-A69B-44CD-8678-573CDF975F57}

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** InstallerProgress
Value: 19

(PID) Process: (3956) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\197218
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {46F36D0A-FE84-4AEA-AEB9-E52EEFAF73D0}

(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	InstallerProgress
Value:	39		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	InstallerProgress
Value:	46		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	InstallerProgress
Value:	53		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	InstallerProgress
Value:	59		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	UninstallString
Value:	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\132.0.6834.116\Installer\setup.exe		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	UninstallArguments
Value:	--uninstall		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	DisplayName
Value:	OneStart		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	UninstallString
Value:	"C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\132.0.6834.116\Installer\setup.exe" --uninstall		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	InstallLocation
Value:	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	DisplayIcon
Value:	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe,0		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	NoModify
Value:	1		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	NoRepair
Value:	1		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	Publisher
Value:	OneStart.ai		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	Version
Value:	132.0.6834.116		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	DisplayVersion
Value:	132.0.6834.116		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	InstallDate
Value:	20250307		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	VersionMajor
Value:	6834		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OneStart.ai OneStart
Operation:	write	**Name:**	VersionMinor
Value:	116		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	name
Value:	OneStart		

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** lang
Value: en

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** pv
Value: 132.0.6834.116

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}\Commands\on-os-upgrade
Operation: write **Name:** CommandLine
Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\132.0.6834.116\Installer\setup.exe" --on-os-upgrade --verbose-logging %1

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}\Commands\on-os-upgrade
Operation: write **Name:** AutoRunOnOSUpgrade
Value: 1

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\CLSID\{A2C6CB58-C076-425C-ACB7-6D19D64428CD}\LocalServer32
Operation: write **Name:** ServerExecutable
Value: C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\132.0.6834.116\notification_helper.exe

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Windows Error Reporting\RuntimeExceptionHelperModules
Operation: write **Name:** C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\132.0.6834.116\chrome_wer.dll
Value: 0

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** DowngradeCleanupCommand
Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\132.0.6834.116\Installer\setup.exe" --cleanup-for-downgrade-version=$1 --cleanup-for-downgrade-operation=$2

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** CleanInstallRequiredForVersionBelow
Value: 85.0.4169.0

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** InstallerProgress
Value: 66

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** InstallerProgress
Value: 73

(PID) Process: (8648) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart
Operation: write **Name:** InstallerPinned
Value: 0

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** InstallerSuccessLaunchCmdLine
Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --from-installer

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** InstallerProgress
Value: 80

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Operation: write **Name:** AppUserModelId
Value: OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** AppUserModelId
Value: OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** ApplicationIcon
Value: C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe,0

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** ApplicationName
Value: OneStart

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** ApplicationDescription
Value: Access the Internet

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** ApplicationCompany

Value: OneStart.ai

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBPDF.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Operation: write **Name:** AppUserModelId
Value: OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBPDF.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** AppUserModelId
Value: OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBPDF.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** ApplicationIcon
Value: C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe,0

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBPDF.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** ApplicationName
Value: OneStart

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBPDF.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** ApplicationDescription
Value: Access the Internet

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\OSBPDF.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Application
Operation: write **Name:** ApplicationCompany
Value: OneStart.ai

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\onestart.exe
Operation: write **Name:** Path
Value: C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\.htm\OpenWithProgids
Operation: write **Name:** OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\.html\OpenWithProgids
Operation: write **Name:** OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\.mhtml\OpenWithProgids
Operation: write **Name:** OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\.pdf\OpenWithProgids
Operation: write **Name:** OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\.shtml\OpenWithProgids
Operation: write **Name:** OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\.svg\OpenWithProgids
Operation: write **Name:** OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\.xht\OpenWithProgids
Operation: write **Name:** OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\.xhtml\OpenWithProgids
Operation: write **Name:** OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CLASSES_ROOT\.webp\OpenWithProgids
Operation: write **Name:** OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM
Value:

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\InstallInfo
Operation: write **Name:** ReinstallCommand
Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --make-default-browser

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\InstallInfo
Operation: write **Name:** HideIconsCommand
Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --hide-icons

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\InstallInfo
Operation: write **Name:** ShowIconsCommand

Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --show-icons

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\InstallInfo
Operation: write **Name:** IconsVisible
Value: 1

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities
Operation: write **Name:** ApplicationDescription
Value: OneStart is a web browser that runs webpages and applications with lightning speed. It's fast, stable, and easy to use. Browse the web more safely with malware and phishing protection built into OneStart.

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities
Operation: write **Name:** ApplicationIcon
Value: C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe,0

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities
Operation: write **Name:** ApplicationName
Value: OneStart

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\Startmenu
Operation: write **Name:** StartMenuInternet
Value: OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\FileAssociations
Operation: write **Name:** .htm
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\FileAssociations
Operation: write **Name:** .html
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\FileAssociations
Operation: write **Name:** .mhtml
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\FileAssociations
Operation: write **Name:** .pdf
Value: OSBPDF.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\FileAssociations
Operation: write **Name:** .shtml
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\FileAssociations
Operation: write **Name:** .svg
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\FileAssociations
Operation: write **Name:** .xht
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\FileAssociations
Operation: write **Name:** .xhtml
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\FileAssociations
Operation: write **Name:** .webp
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation: write **Name:** http
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation: write **Name:** https
Value: OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM

(PID) Process: (7740) setup.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations

Operation:	write	**Name:**	irc
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	mailto
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	mms
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	news
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	nntp
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	sms
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	smsto
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	snews
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	tel
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	urn
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Clients\StartMenuInternet\OneStart.TEKM6WPNRLCWJ4BWL4YY3HFCAM\Capabilities\URLAssociations
Operation:	write	**Name:**	webcal
Value:	OSBHTML.TEKM6WPNRLCWJ4BWL4YY3HFCAM		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation:	write	**Name:**	GlobalAssocChangedCounter
Value:	114		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	FirstNotDefault
Value:	5E030EBD508E2F00		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	InstallerProgress
Value:	86		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	InstallerProgress
Value:	100		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	InstallerResult
Value:	0		
(PID) Process:	(7740) setup.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation:	write	**Name:**	InstallerError
Value:	0		
(PID) Process:	(8852) msiexec.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders
Operation:	delete value	**Name:**	C:\Config.Msi\

Value:

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Rollback\Scripts
Operation: delete value **Name:** C:\Config.Msi\117aac.rbs
Value: 輧Ü

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Rollback\Scripts
Operation: delete value **Name:** C:\Config.Msi\117aac.rbsLow
Value: ▯銳

(PID) Process: (8852) msiexec.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore\Volatile
Operation: write **Name:** NestingLevel
Value: 0

(PID) Process: (8852) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation: delete value **Name:** Sequence
Value:

(PID) Process: (8852) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation: delete value **Name:** SessionHash
Value: 恧蒼赧曊ᴛc¬汗

(PID) Process: (8852) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation: delete value **Name:** Owner
Value: ⊔

(PID) Process: (8852) msiexec.exe **Key:** HKEY_USERS\S-1-5-21-1693682860-607145093-2874071422-1001\SOFTWARE\Microsoft\RestartManager\Session0000
Operation: delete key **Name:** (default)
Value:

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\StabilityMetrics
Operation: write **Name:** user_experience_metrics.stability.exited_cleanly
Value: 0

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart
Operation: write **Name:** UsageStatsInSample
Value: 1

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** usagestats
Value: 0

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid
Value:

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid_installdate
Value: 0

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid_enableddate
Value: 0

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** extensions.ui.developer_mode
Value: 37B859FC616C47C396331F3FC1D9BA17835B8484F837F55F806FE1C020DD890B

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** google.services.last_signed_in_username
Value: 757CFEBCD9B0B29F2606735EA86823C2CDD92CD76E8EE950C507FB0778DB914B

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** media.cdm.origin_data
Value: 806FC6108C9C6CE5083FBA32142CB9EA8F419AA5546B3C079CA642CC2E1C4650

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** media.storage_id_salt
Value: CA1DDE54259E5D5EEA618B03652520CE9BAE5BEFA4D30FCED2A117E0A93431A3

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** google.services.account_id
Value: 501DA0EA15D6ACEBF92314826D7B8C7E53DEF21356B532E60B5EF744FB65C338

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** default_search_provider_data.template_url_data

Value: B415DF9B6EE52FE9695FD1A2CB029AD7F34743A081D56804665C4DD9361C9137

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** safebrowsing.incidents_sent
Value: D89B20B82E784153EDAD9477A2BEFFF4F793F4B95591685430A36F286D3FB3AB

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** pinned_tabs
Value: FDE43BC86643A6DC3D27DFDBE37AB40C323D2245C06A659A982D060900C77B59

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** search_provider_overrides
Value: 8D8243F860A767A1B1676EFA7EDA66200BBC838A140973A052334F170292E31A

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** prefs.preference_reset_time
Value: 73DD4ED2288514F08089D764D8BD4246D6F00E9E8F8416B2270453BB2B7FBA5F

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** google.services.last_username
Value: 4034EE8966D5F3E4FAA7276B3804166652AD9233368746577800CA338B757742

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** session.startup_urls
Value: E4A90BEEA35642A9D68F720F763239781FA2CB59906F27C26830285ED6777303

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** session.restore_on_startup
Value: 9C5892478BC56BF747881DDB1D2B9557B4A2ABB3A6681797BE1B93824D7A8FBE

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** browser.show_home_button
Value: FFD747F9F75522EE9885D830257F63E2372B9465D4B461A373F196CC60036D62

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** homepage
Value: 0C4F32A029F6C6251F2D680FA8EA1411E8098B30A108EACB4F63C2E7C1EC8BB5

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** enterprise_signin.policy_recovery_token
Value: D180C477BDDED209326201224ECDD813192DADC30E6B090C318FAD279A320F55

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** homepage_is_newtabpage
Value: 89CD48B62183279997EE3831BD4D12742A9E713F4C5A3618AC6D9CBEA7B69808

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation: write **Name:** GlobalAssocChangedCounter
Value: 115

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation: write **Name:** GlobalAssocChangedCounter
Value: 117

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation: write **Name:** OneStartChromium
Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --existing-window

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation: write **Name:** OneStartUpdate
Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --update

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation: write **Name:** GlobalAssocChangedCounter
Value: 116

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** lastrun
Value: 13385801331893590

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\BLBeacon
Operation: write **Name:** version
Value: 132.0.6834.116

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\BLBeacon
Operation: write **Name:** state

Value: 1

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\BLBeacon
Operation: write **Name:** failed_count
Value: 0

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** dr
Value: 1

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation: write **Name:** OneStartAutoLaunch_038081DD5A6579E473F75821B3C4462D
Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --no-startup-window --from-registry /prefetch:5

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation: delete value **Name:** OneStartAutoLaunch_038081DD5A6579E473F75821B3C4462D
Value: "C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe" --no-startup-window --from-registry /prefetch:5

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: delete value **Name:** default_search_provider_data.template_url_data
Value: B415DF9B6EE52FE9695FD1A2CB029AD7F34743A081D56804665C4DD9361C9137

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: delete value **Name:** extensions.settings
Value:

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** default_search_provider_data.template_url_data
Value: F7E4D8F31474931C297FF95797861E33F81E7B0781A054619179638EAC93B2B7

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** ahfgeienlihckogmohjhadlkjgocpleb
Value: 96C313785328D7C227045F2826BCC95BA8D2664BD50393AA187055BEC6EAED53

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** memhbiihnoblfombkckdfmemihcnlihc
Value: B0B28D17726A46EDB33A0C7306E8869E2BF6C4FEB56CC8CAE5F860073C4282D4

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default\extensions.settings
Operation: write **Name:** mhjfbmdgcfjbbpaeojofohoefgiehjai
Value: 80126C5E7E1EB42B80FACEC917DF3097B5C496C62DD3E2E194389887C2E1385E

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: delete value **Name:** pinned_tabs
Value: FDE43BC86643A6DC3D27DFDBE37AB40C323D2245C06A659A982D060900C77B59

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\PreferenceMACs\Default
Operation: write **Name:** pinned_tabs
Value: D4943455A7EB06F4E343F409769BB2BDE61286624B63B1E774CF54F0A9D7FB9E

(PID) Process: (8696) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\BLBeacon
Operation: write **Name:** failed_count
Value: 0

(PID) Process: (8696) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\BLBeacon
Operation: write **Name:** state
Value: 2

(PID) Process: (8696) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\ThirdParty
Operation: write **Name:** StatusCodes
Value:

(PID) Process: (8696) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\ThirdParty
Operation: write **Name:** StatusCodes
Value: 01000000

(PID) Process: (8696) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\OneStart\BLBeacon
Operation: write **Name:** state
Value: 1

(PID) Process: (1280) onestart.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\OneStart.ai\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** lastrun
Value: 13385801362741970

(PID) Process: (6736) ShellExperienceHost.exe **Key:** \REGISTRY\A\{ed477523-7a4e-c859-2e82-5d5242e8370a}\LocalState
Operation: write **Name:** PeekBadges

Value: 5B005D000000583D6C86278FDB01

Files activity

Executable files	Suspicious files	Text files	Unknown types
72	980	217	4

Dropped files

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old~RF10b2d7.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old~RF10b2f6.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old~RF10b2f6.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old~RF10b2f6.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old~RF10b2f6.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old~RF10b2b8.TMP **MD5:** C5C8E14929BCE261B2B5B899CB479AF7 **SHA256:** 73DBFF8A366CFF6972A38C091782EF62C89E28FDA1423A47448A60343F921754	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old **MD5:** 798EBA8558D3655BC5D2B61984B3BF12 **SHA256:** 04EB76D36567C4FD801C5583AA34A18A081D9030BAE3034D8F81D419A797221D	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\fa2fa077-3fe0-474f-a663-53a4122dc4d1.tmp **MD5:** 4EA7802B635FFD88E798768CDD55481C **SHA256:** 570B4062C8C2C054C964697804E25FE3E538262461708E3DDFD760B4A4541C84	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\3c2ea39a-31fb-4705-86b9-e1267e5642ae.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Variations **MD5:** 6971E42ED64D2BE125547F021EB852B1 **SHA256:** B46CFDC4106DF566F71AA34D6F10B53767C561DFD17DD07A5930A18E67BB344B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF10b354.TMP **MD5:** 4EA7802B635FFD88E798768CDD55481C **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\settings.dat **MD5:** 1E9E15EF6E531C4557100F20C9C76F01 **SHA256:** 46CB063CC268B69B172660F166C4394D5B4EDD802388B3EC16766DEBDB9F86C3	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF10b298.TMP **MD5:** 1051384B8864AC718AE413E9B1D309A5 **SHA256:** 3FC536607727B6030F7B4714D6E03B4CA040B2EBDBE81B74538F345432207360	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old~RF10b2b8.TMP **MD5:** 92941BAD29B823669F85E6F7352F04EB **SHA256:** 19E674BF425E68E8B1C1242017BB22044BA558B1D5644F5D4EBA973AF39BABAA	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old~RF10b2f6.TMP **MD5:** 818E5512B63AF7BC7B8363A92D905712 **SHA256:** ECD4298AE18D0B60EA5F0B3B04761F740B51B18B0D69B42CEF028463A7A46780	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Version **MD5:** C7E2197BAE099B13BBB3ADEB1433487D **SHA256:** 3460EEAF45D581DD43A6E4E17AF8102DDAFF5AEAA88B10099527CF85211629E9	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old~RF10b3d1.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old **MD5:** — **SHA256:** —	—

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index **MD5:** 01F0B29822F7C00694ABF3150276196A **SHA256:** C5CA04147E678498F16E8DED9EFB227591ABF40A3AFC5E65248D019D9B9198D9	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\06fa14b9-11b7-41cd-afc6-12c560f25b48.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\temp-index **MD5:** 01F0B29822F7C00694ABF3150276196A **SHA256:** C5CA04147E678498F16E8DED9EFB227591ABF40A3AFC5E65248D019D9B9198D9	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old **MD5:** FF65CBE0D511D23B79B630DD40BA28B6 **SHA256:** 0BAFE077764110A681D8E15801BDAA10395BCFE9087FFF703BA3A83CAF73ADF0	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State **MD5:** 4EA7802B635FFD88E798768CDD55481C **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\07e7caf2-0685-4b85-a7b7-6dfc9f8361ad.tmp **MD5:** 86A581376460D1DE379EA1CDE245C48A **SHA256:** CA616A6D3113B502FBD7A4EAD0AAA7FF59BEF628D554F70FF3D091FB5A1B99AF	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old **MD5:** 1AF1D1ED27A40F9FDA977B6C353EC48B **SHA256:** 01B66ED195749BF7909E0B655A6C4C6AFDECD665D7304653D09CD538191CC50A	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old~RF10b3a2.TMP **MD5:** 29F7449691899E3CFC14F94670812757 **SHA256:** 1D1DF03022CD740C76320CAC538DE55D4521FF4EA32CE83275C982F1B308BBC6	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\todelete_e13a8db1ed224228 **MD5:** 95FC65CACF599A197741EB36DEB0F8AE **SHA256:** B84BDA5415D69DA598F2015A9BFDB024727F3DE3F0E9E6B16FDD7533026A5565	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\arbitration_service_config.json **MD5:** 350ABC86EFB653D78BE8F2FA5D7BDB8C **SHA256:** C42FB154D987390FCCC0F63DAFCED2BA7242410BADF64D6FF5FDC2FB26D103C9	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\a74ec3b60a5ce565_0 **MD5:** B54F76986107E40DA3B0D7743D5D0CAF **SHA256:** 17B5347C05B71F51151A6720137C617E0B29DB34B28528F4A35B2E144FD84B0D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\e0495fde257df2ef62ee7e3fdb1ebb9d7ff72300.tbres **MD5:** AE21D088F7D99279EF22FA58E9C5FE0D **SHA256:** 810C9BEEFCF6F3816984A64A9C5177CB3C4BF5D09E2A4A739C8A71228AFA71B8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old **MD5:** D95248482054CC3F9158A60D13CE0BCE **SHA256:** AF8C73D6599B0D7603D52E50A01CD7A6AF4F3D23C5023CDF26B81DC0C14E0609	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old~RF10b567.TMP **MD5:** 35D729BE231A18224EB4469BA4BAB0E3 **SHA256:** 0D5F32F9C261450E1EAD9B4B12A3CD580C93389D11EB5CB5EC373950D6AC87FE	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old **MD5:** 7959D8DB0CBADD0EA4A5F1CC4E5B5138 **SHA256:** 270CB1734B667CF46D5A0A3149F36BC8867E5A239B56B212908994381528CD59	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000258 **MD5:** BD00156E977BB9F95D8C857DD8CA3D72 **SHA256:** C0942123FE20B22F41A86E2D5BAC6274C20CE6E4D24B59A591FC702B624FA065	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports~RF10b9dc.TMP **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\load_statistics.db-wal **MD5:** D7A4A9D41CFB6F4ABEF9A38E4B4429FC **SHA256:** 31A33230C731B24A081B7EA855E5AE24BAE4E2B1C9644AE834E83AD47608272E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\e8ddd4cbd9c0504aace6ef7a13fa20d04fd52408.tbres **MD5:** C413F2CB07713B8F6E3C2179B9EF4DE1 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old~RF10b4ea.TMP **MD5:** A913CE23AF5CEF8D1CD91F60B37EFA59 **SHA256:** A84AD219E5E1144AE35FACE15704BD066CCA689BECD82500276C7A6C5484F82D	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old~RF10b4ea.TMP **MD5:** C1C75CFDA95DA438E30077FF767A6FDF **SHA256:** CED5E0654E5732FDDB0AE882D981C3FA7171889874047821BDF00245DC8EA913	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\default_cloud_config.json **MD5:** 18261EB12378081F939FB9415CA0C9E1 **SHA256:** 12BBEEC9A0AF9E3ED945B28B9B8EF89B2F897768D1BA3FFD6F3FBB42FA5BC556	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old~RF10b4bb.TMP **MD5:** CE118DF5F2969D979F3D0E779BACF798 **SHA256:** 830316C00FB44CBFCC6AFF55FBE014BAA63B20B9BAA1DCE9E43856911F4F357E	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old **MD5:** BB2F8FF0F266CFB047C8472B2ED83BA2 **SHA256:** A8A372371A7E0DCDD0CF009BB5A4C6B192DBE0D83408EA91251A8185790236C1	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old **MD5:** A440B2B4E06AF56BCDC8AE0E4ABF7A0B **SHA256:** EE6899D4DEE495E71C452A696AE4C984ED4DA5BF5E43078BF5EF10210F95D318	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000259 **MD5:** A2F0EFB299A2A5F50B4F18E2F810BA52 **SHA256:** DA58C44BB91DFDF5DE267D852A468B9CBD3052A00BCB0A90F9D03D1A988F9E53	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\ed31d47468720347_0 **MD5:** E4ABFDE9AB5904EDC86E83F2C1DC386C **SHA256:** 5C82F26177320BFE84B16D801253728E56013732EAF8E61F61C61537B61139E7	binary

PID	Process	Filename	Type
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025f **MD5:** 9B512DA1FC588A609A15EFDA1E6B83D6 **SHA256:** 951E4764C1CB7ABB3582C9F32C8950460DE95401F5D0A515005C3A7C20488DC4	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\324ca58de33dccb3_0 **MD5:** C3722923CFB21027583FAC54B3E215C1 **SHA256:** 4A677B723FF5CE1D41FE421EF23E695BB970E694141C7418ECB3A3C7309BEB40	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5a2a7058cf8d1e56c20e6b19a7c48eb2386d141b.tbres **MD5:** 64D4C1581B4EA4FF89687DF6D98B5FF2 **SHA256:** 90F4AF6CB47096C0E891E190243BF55D5BB15D04E5114C091B7479562C95CE96	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025b **MD5:** C8EC290DD651916352F97F3D8270ABD5 **SHA256:** 2B9C0E305A89862F5BA54D3817CA5407ADBC677D754EE17B6DD8760F82A1F144	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025a **MD5:** 015C126A3520C9A8F6A27979D0266E96 **SHA256:** 3C4D6A1421C7DDB7E404521FE8C4CD5BE5AF446D7689CD880BE26612EAAD3CFA	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\42a4a455-e03e-410a-a627-3e8d1127cac6.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025c **MD5:** A2F0EFB299A2A5F50B4F18E2F810BA52 **SHA256:** DA58C44BB91DFDF5DE267D852A468B9CBD3052A00BCB0A90F9D03D1A988F9E53	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\94ba874e-a7f6-407c-b55c-add8afd8584b.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports~RF10b8e2.TMP **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\e466735edebcaec3_0 **MD5:** AAD40481FF49EF9033074371458C32C9 **SHA256:** 4B1999EE7EE91486C1C338D74D39E03595C3D1627C5020BCC83E20A5A4D193F7	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old **MD5:** 8C15B19DD1169F3CA1A561CAFD619C02 **SHA256:** 0A69BB99412A7E4F7205F73AEDD9AB5D810D1639967F441AD8F711E702C53C0F	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000262 **MD5:** 9D8BED950DFF45423B367BBEAD952789 **SHA256:** EE13B2E6C137230339B2BE508003AD0C3AA898D389AC969CBABCF1E7F559AAE4	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025e **MD5:** D17B5A55EC9D8608C1D2B531CCB6DE88 **SHA256:** DC2A3600C7CDFAEA40DB03757D6915D67518215DB51397C8A5BB3F132AE89A49	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000265 **MD5:** B34C8A2DD0150CDA2C245923B833B873 **SHA256:** —	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000264 **MD5:** DFE94051125F76CA0BB1200A444B0149 **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000266 **MD5:** 0378815D113388B4CDFBC1D20DFD46BF **SHA256:** B49B2C8A7846FB18709F3D2DF1062796F55BEC9C7B9674B7BBDF2108D3AAA68E	executable
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old~RF10cdf0.TMP **MD5:** F22D72EFC12605BD6816B1F8B7831571 **SHA256:** D2442EFEB93BB5FD6FCFBA845320E097340EE086F48B1615484815BBA82BE122	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000260 **MD5:** D743E72F71B45E4F1EDEE8ED47A6E2C1 **SHA256:** 1B8B874E1763A59ABAC3C8B03F905C8E7CDE9B7DE998C230727A6150303E7725	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_model_metadata_store\LOG.old~RF10d1f8.TMP **MD5:** — **SHA256:** —	—
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025d **MD5:** 9B512DA1FC588A609A15EFDA1E6B83D6 **SHA256:** 951E4764C1CB7ABB3582C9F32C8950460DE95401F5D0A515005C3A7C20488DC4	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_model_metadata_store\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old~RF10d207.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\db3e640539bcc1ba_0 **MD5:** 0567360D60FDA475703DC1AA063CFD34 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old **MD5:** 90E7FBA78823C029EB63EEBE05CB6647 **SHA256:** C402019AD51200620B9C3040D984A4EC6FF336CFB22039E29B761BE2DD63ADEE	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old~RF10d255.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old	—

PID	Process	Filename	Type
		MD5: — **SHA256:** —	
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000263 **MD5:** 8E08464E9F4721C08DB8B484718E8B45 **SHA256:** BD2C404DE1030BE8C6C8B8FC1FF66E21AECD509F060056D17B31F3EDBB1A6E19	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old~RF10d255.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\Downloads\08883af5-72a4-48d4-a0d8-d7c49e817680.tmp **MD5:** FE7B0742AAA35D7F4D04E8ACB947A2BF **SHA256:** 73ED308345A64520B2CE295691008C131F48B7AD4E1F0F6911B811E4E7A45633	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old **MD5:** 5F3EEB8D3062277537ADC926892A6E0A **SHA256:** 601234D6C9DE44AE76920A3FD2E7D5C21F01C65CE8778BC084D02D977A801581	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\fca04a3f-7664-437f-8dee-2ad901728105.tmp **MD5:** 4A164D87B3F685E409A55B31861F0AE2 **SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old **MD5:** BD715F079C51E8C4D9AADFEF70125BD9 **SHA256:** 3DDC987F3DD33EA96D8B1D4E805E3A2D3B84B44C5F8FF0F224791F3ABFE7EDD7	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old~RF10cd83.TMP **MD5:** 1F7041F0A707168BF7733D1A2047492C **SHA256:** DB748A5163B0AB1FF8F312BC376F6BC8F5F4907BBC6DC85ED07299C656F2F729	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000261 **MD5:** 8E08464E9F4721C08DB8B484718E8B45 **SHA256:** BD2C404DE1030BE8C6C8B8FC1FF66E21AECD509F060056D17B31F3EDBB1A6E19	image
8100	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\domains_config.json **MD5:** 654361DE6EB03989B7010CF01CAF9F86 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\Downloads\Unconfirmed 864943.crdownload **MD5:** FE7B0742AAA35D7F4D04E8ACB947A2BF **SHA256:** 73ED308345A64520B2CE295691008C131F48B7AD4E1F0F6911B811E4E7A45633	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139\dasherSettingSchema.json **MD5:** 4EC1DF2DA46182103D2FFC3B92D20CA5 **SHA256:** 6C69CE0FE6FAB14F1990A320D704FEE362C175C00EB6C9224AA6F41108918CA6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old~RF10cde1.TMP **MD5:** 279162E139C357A4BBCFBCFDD7A00E88 **SHA256:** 6B09138C2640F10EE9B088C48A47210A8570C7DCB3CAF340BADE94AC97FE9A0A	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\cv_debug.log **MD5:** D1D7A57CBCDBD87F2D0DA2A039C5C52E **SHA256:** 631922270552D31D3714271E3B261FF92558422BD2D1328DE4358B4A4223BC54	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000267 **MD5:** 0E6652994F4DDA1B8980A7EBD3B5A7E8 **SHA256:** 93CC94D9696C6FF0BBE4BF2657654C25A805BF8F9E154035CB1AFC9CEAEC7561	compressed
3956	msedge.exe	C:\Users\admin\Downloads\smartonestartpdf.msi **MD5:** 0378815D113388B4CDFBC1D20DFD46BF **SHA256:** B49B2C8A7846FB18709F3D2DF1062796F55BEC9C7B9674B7BBDF2108D3AAA68E	executable
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Browser **MD5:** A397E5983D4A1619E36143B4D804B870 **SHA256:** 9C70F766D3B84FC2BB298EFA37CC9191F28BEC336329CC11468CFADBC3B137F4	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139\page_embed_script.js **MD5:** 0396274AAF2EAE8917E5EB52CF69DFA4 **SHA256:** 13E1562CD07FC06D692FDF1AA471E3CEAE3CF7C1E42C5345D430A947139A24D5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps~RF10ceac.TMP **MD5:** 4A164D87B3F685E409A55B31861F0AE2 **SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\msedge_url_fetcher_3956_969784574\GHBMNNJOOEKPMOECNNNILNNBDLOLHKHI_1_89_1_0.crx **MD5:** EAE462C55EBA847A1A8B58E58976B253 **SHA256:** EBCDA644BCFBD0C9300227BAFDE696E8923DDB004B4EE619D7873E8A12EAE2AD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps **MD5:** 4A164D87B3F685E409A55B31861F0AE2 **SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\sw\messages.json **MD5:** 84EB1D6E827E40C578469EAAB778E368 **SHA256:** 2C6B42D122943DC0CA92A33074D1A607351D3BC7F9768E174617FA7011A3DE9F	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\fil\messages.json **MD5:** F954B2E970DC96E5889499DB7392FD59 **SHA256:** 41CE6A7B18364EFECCED0419B42165D4F86C43643BBE1043014D4142CF86186A	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139\manifest.json **MD5:** B0422D594323D09F97F934F1E3F15537 **SHA256:** 401345FB43CB0CEC5FEB5D838AFE84E0F1D0A1D1A299911D36B45E308F328F17	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\km\messages.json **MD5:** B3699C20A94776A5C2F90AEF6EB0DAD9 **SHA256:** A6118F0A0DE329E07C01F53CD6FB4FED43E54C5F53DB4CD1C7F5B2B4D9FB10E6	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\de\messages.json **MD5:** 5DAF77AE7D2B7DBEF44C5CF7E19805EE **SHA256:** 22E2828BFDBB9C340E7806894AE0442BD6C8934F85FBB964295EDAD79FD27528	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\lt\messages.json	binary

PID	Process	Filename	Type
		MD5: 8047409DCC27BFCC97B3ABCE6DAB20EF **SHA256:** B42EBFE071EF0EC4B4B6553ABF3A2C36B19792C238080A6FBC19D804D1ACB61C	
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\fi\messages.json **MD5:** 1D4778E02337674D7D0664B5E7DFCBBE **SHA256:** A822B0E66D04644D1CFBD2517736728438743162C3213F15D986E2DB85BD0213	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ne\messages.json **MD5:** 065EB4DE2319A4094F7C1C381AC753A0 **SHA256:** 160E1CD593C901C7291EA4ECBA735191D793DDFD7E9646A0560498627F61DA6F	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\sr\messages.json **MD5:** C2026342237E7686B1932AF5B54F8110 **SHA256:** A3EB276FBD19DCE2B00DB6937578B214B9E33D67487659FE0BF21A86225ECE73	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\sl\messages.json **MD5:** 9CDFA5371F28427F129D200338C47494 **SHA256:** 75D018CC8525605DDC591F6BFE5BDAA2EFB164934E9D5438972651F8C818D581	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139\offscreendocument_main.js **MD5:** 01984DBFE92DF14DBD118C381A3D48F4 **SHA256:** 3A78B6FBC16F9FB27CE3ED650ABC31174263D762B71C028CC5D8F5427CBAB082	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\en_CA\messages.json **MD5:** 558659936250E03CC14B60EBF648AA09 **SHA256:** 2445CAD863BE47BB1C15B57A4960B7B0D01864E63CDFDE6395F3B2689DC1444B	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\nl\messages.json **MD5:** D448E11801349AB5704DF8446FE3FA4C **SHA256:** E98C5CFE277A338A938E7277DEEC132F5EA82A53EBDB65FF10E8A2FF548AC198	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139\service_worker_bin_prod.js **MD5:** BC4DBD5B20B1FA15F1F1BC4A428343C9 **SHA256:** DFAD2626B0EAB3ED2F1DD73FE0AF014F60F29A91B50315995681CEAAEE5C9EA6	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\es_419\messages.json **MD5:** 94BC2D5609F6D670E181E1FF0D041869 **SHA256:** E848603B7A73A88E3FE7BFFA20E83397F5D1E93E77BABB31473CC99E654A27B7	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\el\messages.json **MD5:** 32886978EF4B5231F921EB54E683EB10 **SHA256:** 728D8CBD71263680A4E41399DB65B3F2B8175D50CA630AFD30643CED9FFE831F	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\en\messages.json **MD5:** 558659936250E03CC14B60EBF648AA09 **SHA256:** 2445CAD863BE47BB1C15B57A4960B7B0D01864E63CDFDE6395F3B2689DC1444B	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\es\messages.json **MD5:** 59CB3A9999DFBD19C3E3098F3B067634 **SHA256:** 02168993A23E074E0800CBB338FE279F99EF420E326BF92916FFED83C1F06533	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\te\messages.json **MD5:** 50AB4DEABAD394D13C265B8B80D9F9C3 **SHA256:** 90868A8A4A4DBF48770C14A161FAEA406EF9A453B75F4CB7A53C1B4E96A88599	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\eu\messages.json **MD5:** 29A1DA4ACB4C9D04F080BB101E204E93 **SHA256:** A41670D52423BA69C7A65E7E153E7B9994E8DD0370C584BDA0714BD61C49C578	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\en_GB\messages.json **MD5:** C4E77421F3361277F7E3AA3472B5EB10 **SHA256:** C7255E9B784C4B8DF7DF7B78F33A5737A9AB7382F73465351597B1DA9B3D5FE7	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\et\messages.json **MD5:** B18007BFC2B55D2F5839A8912110B98D **SHA256:** 7CCC7B17BFE01C3C7DD33EFF8F80D0B57FC9B175815E766C9C1C1E893725E20F	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\fa\messages.json **MD5:** E578E08EE604158D674982BA060396FD **SHA256:** E758273C25FBAD804FE884584E2797CAEFBBD1C2877DFD6F87AB1340CD25252E	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ta\messages.json **MD5:** 24626AD7B8058866033738380776F59B **SHA256:** 3FC7F56F6D6D514B32547509B39F6380FC786EFBCCA4B9859F204456CA2E7957	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RF10d35f.TMP **MD5:** — **SHA256:** —	—
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\zh_TW\messages.json **MD5:** B571E4CEFD96A2651FFB6621C4D3D1B4 **SHA256:** 16B8F7BE42B982D5AD9F638E71DA38D134394B9BAB9255F73CF514ABBFAAF146	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old **MD5:** — **SHA256:** —	—
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\az\messages.json **MD5:** C603747B8578C1324DD262565F643E06 **SHA256:** 614470DA3C5034ACE649F1786BEAAAD2C94F4475BCC8858390B721F06FB7BF64	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\cy\messages.json **MD5:** A86407C6F20818972B80B9384ACFBBED **SHA256:** A482663292A913B02A9CDE4635C7C92270BF3C8726FD274475DC2C490019A7C9	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\en_US\messages.json **MD5:** 64EAEB92CB15BF128429C2354EF22977 **SHA256:** 4F70ECA8E28541855A11EC7A4E6B3BC6DD16C672FF9B596ECFB7715BB3B5898C	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\da\messages.json **MD5:** 0E451C9C8453577E513AABF630C275F2 **SHA256:** 94CDDB998C2C5AB40B6F074C359A60E6EEBAAA2D52A9649C22F4EA4C1B9936F2	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\gu\messages.json **MD5:** 86DE754C2D6B550048C9D914E55B5FF0 **SHA256:** CC3E9077FCC9BD0DFC5DD3924C6C48B8345F32CEE24FCCC508C279F45B2ABE61	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ru\messages.json	binary

PID	Process	Filename	Type
		MD5: F70662272A8FC9141A295A54002F644F **SHA256:** DF379187B7F6DE700E5C53420336E6B31B7DC31015F77B2B256256BCF9BE54B7	
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\hu\messages.json **MD5:** FB8D08676AA88683F27A2759C5837529 **SHA256:** CF26310B073B0891996ECD761C6CB53F00193DEE524213A9FB34225D636EC4B7	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ja\messages.json **MD5:** 113A674F2E4C66CC4D2A9C66ED77ADEA **SHA256:** C1094A1D8457E782F229910B70FC7AECE356AA779A423E869104946814660D35	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\hi\messages.json **MD5:** 4A9C9F947B479E5D89C38752AF3C70EA **SHA256:** 14895BF43CE9B76C0FF4F9AEF93DBE8BB6CA496894870CF0C007B189E0CEF00E	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\bn\messages.json **MD5:** B1101FAC65CE2FAA3702E70FD88957D2 **SHA256:** 3E3CEAA214D8079B02C9C941635F5D45E621236D9C3F82E06AC604F0772670E8	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\mr\messages.json **MD5:** 34CE3FA84E699BCE78E026D0F0A0C705 **SHA256:** 275E7FADB93A810328E3ADEAD8754DD0A19A062D5D20A872F7471FFAB47AA7B3	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\pt_PT\messages.json **MD5:** AA431EC252B4339A49D172C6B9292BA3 **SHA256:** 156FC7BA9B5728908E1A74950B97474F73D8F58933D345C8EEEA8284565C8357	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\zu\messages.json **MD5:** 71F916A64F98B6D1B5D1F62D297FDEC1 **SHA256:** EC78DDD4CCF32B5D76EC701A20167C3FBD146D79A505E4FB0421FC1E5CF4AA63	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RF10d3bd.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old **MD5:** — **SHA256:** —	—
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\si\messages.json **MD5:** B8A4FD612534A171A9A03C1984BB4BDD **SHA256:** 54241EBE651A8344235CC47AFD274C080ABAEBC8C3A25AFB95D8373B6A5670A2	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\fr_CA\messages.json **MD5:** 681422E3FCF8711AF8EEFBB75A607C8E **SHA256:** AF889C1DEB6F9248961C2F8BA4307A8206D7163616A5B7455D17CEAD00068317	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\zh_CN\messages.json **MD5:** E910D3F03F0349F5C8A6A541107375D5 **SHA256:** 3893C066A36FE95F06F3C49091A20290D4E071183755F40AF05455660BEDA2DC	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\my\messages.json **MD5:** 342335A22F1886B8BC92008597326B24 **SHA256:** 243BEFBD6B67A21433DCC97DC1A728896D3A070DC20055EB04D644E1BB955FE7	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ms\messages.json **MD5:** DB4D49231C88C11E8D8C3D71A9B7D3D4 **SHA256:** 9B32C491D0BFEBDCA1455F73C3C6F71796D433A39818C06C353DA588DE650F81	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RF10d3dc.TMP **MD5:** — **SHA256:** —	—
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ml\messages.json **MD5:** CE70315E2AAEDA0999DA38CC9FE65281 **SHA256:** 907F2709D1D3C8FA26294938F4080BC477E62281C4C50A082C22DB0195CDA663	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\is\messages.json **MD5:** CAEB37F451B5B5E9F5EB2E7E7F46E2D7 **SHA256:** 943E61988C859BB088F548889F0449885525DD660626A89BA67B2C94CFBFBB1B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old~RF10d3dc.TMP **MD5:** — **SHA256:** —	—
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ar\messages.json **MD5:** C825621044E4D5C504404DAE9752285C **SHA256:** 47652115CBB912907F405992FCFC64F987642158F0CB35C9D6E0D4742D833802	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old **MD5:** — **SHA256:** —	—
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\sk\messages.json **MD5:** A46E08B45BE0532E461E007E894B94F4 **SHA256:** 5E886E7B616FBFF3671DAB632D1B6D8DCEEFF9004218485F1B911DCD8C9694A3	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\hy\messages.json **MD5:** 55DE859AD778E0AA9D950EF505B29DA9 **SHA256:** 0B16E3F8BD904A767284345AE86A0A9927C47AFE89E05EA2B13AD80009BDF9E4	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ur\messages.json **MD5:** F6E8FCA4FD1A7AF320D4D30D6055FA6D **SHA256:** 504549057A6A182A404C36112D2450864A6CB4574CD0E8F435CA556FAC52AB0A	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\pt_BR\messages.json **MD5:** 8E24EC937237F48AC98B27F47B688C90 **SHA256:** A6AD5D5FB7C90736E04F898970D2CC9D423415B54B8E572F18C05D6EBAF46F68	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\sv\messages.json **MD5:** F008F729147F028A91E700008130DA52 **SHA256:** 5F4229D18E5606330146EE13BDF726E10C1E06CBB15368C47F1AE68ABE9CE4BA	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\hr\messages.json **MD5:** EB6C5133C1FE7F9E8E4449A917D185D9 **SHA256:** 985976B776E729835E047C81D3D731A6C488A6459AA8918DBC8EC808C0BF73A1	binary

PID	Process	Filename	Type
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\gl\messages.json **MD5:** CC31777E68B20F10A394162EE3CEE03A **SHA256:** 9890710DF0FBF1DB41BCE41FE2F62424A3BD39D755D29E829744ED3DA0C2CE1D	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\fr\messages.json **MD5:** 85718FE4820C674C5305D33DFB5CBDDC **SHA256:** 6713B69B6C9E80B03E0A9D4A7D158197B0C7EC8A853C64C0AF0B1A05CE54D74C	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\bg\messages.json **MD5:** 361B516EDF253851044DAE6BAD6D9D6F **SHA256:** 22BC37B47CE8A832F39701641DC358357676E9BE187A93A4C5D4B016E29238AE	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\kn\messages.json **MD5:** F55CE2E64A06806B43816AB17D8EE623 **SHA256:** 5FA00C465C1C5EED4BEA860CEB78DA9419EA115347BA543DDB0076E5C188FEED	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\af\messages.json **MD5:** 7BC8FED14870159B4770D2B43B95776B **SHA256:** AA12205B108750CF9FA0978461A6D8881E4E80DA20A846D824DA4069D9C91847	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\it\messages.json **MD5:** 88A9ACD41521D1D00B870E2DA3044A88 **SHA256:** 3377A873DB531113D79919E7A89369A79A602BAC6AE09B9864B9378DC285F345	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\lo\messages.json **MD5:** E20D6C27840B406555E2F5091B118FC5 **SHA256:** 89082FB05229826BC222F5D22C158235F025F0E6DF67FF135A18BD899E13BB8F	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\zh_HK\messages.json **MD5:** 524E1B2A370D0E71342D05DDE3D3E774 **SHA256:** 30F44CFAD052D73D86D12FA20CFC111563A3B2E4523B43F7D66D934BA8DACE91	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\no\messages.json **MD5:** 66439BA3ED5BA0C702EF94793E15DE83 **SHA256:** B3ECE279943B28C8D855EC86AC1CE53BDFB6A709240D653508764493A75F7518	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\tr\messages.json **MD5:** 3104BCD0D4AD6B47FE36F36C1B5AA333 **SHA256:** AC2894CEA6332450095A7F8FC9B97550DA87E4B4B6E6FB95DF1A1F49F25E0E35	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\lv\messages.json **MD5:** 20FA89BA92628F56D36AE5BD0909CB15 **SHA256:** 80D64F03DC2CC5283FAF1354E05D3C3CB8F0CC54B3E76FDAE3AD8A09C9D5F267	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\uk\messages.json **MD5:** AE938164F7AC0E7C7F120742DE2BEB1E **SHA256:** 08978A1425DEC304483BBB7DD0E55A7D850C4561ABD41BAC1BE5D93D70465174	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\id\messages.json **MD5:** 3FEFE403F5F537D9A2D28AB36B2C1A94 **SHA256:** 35872A3343D4B4768FE4702A8DC18B749933E81210DB13466AD172BD2880F6EB	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ka\messages.json **MD5:** 83F81D30913DC4344573D7A58BD20D85 **SHA256:** 30898BBF51BDD58DB397FF780F061E33431A38EF5CFC288B5177ECF76B399F26	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Platform Notifications\LOG.old **MD5:** F8F8200E9DC617B01F93320DA6BB7870 **SHA256:** 9FD3E46AB3D926076563DBB90176D38DD5F1427DCD851AF539B019CA62BE9FB9	text
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\iw\messages.json **MD5:** 26B1533C0852EE4661EC1A27BD87D6BF **SHA256:** BBB81C32F482BA3216C9B1189C70CEF39CA8C2181AF3538FFA07B4C6AD52F06A	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ro\messages.json **MD5:** EE122CF26EBE1AD0CC733B117A89FF3B **SHA256:** 4ECEDB9C1F3DD0D0E3AEB86146561B3D7E58656CBDBED1A39B91737B52EC7F2C	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\cs\messages.json **MD5:** 48663A88DCF0EF6C9FADE9BEE4935B91 **SHA256:** 5A701D67910BA6C7CCEDC26E02FA707CC86A1BE57CD7D36290A3D268732A42C7	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ko\messages.json **MD5:** E71A91FE65DD32CAC3925CE639441675 **SHA256:** 57F81A5FCBD1FEFD6EC3CDD525A85B707B4EEAD532C1B3092DAAFD88EE9268EC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Platform Notifications\LOG.old~RF10d41b.TMP **MD5:** 0BFBF23732791ECBD0B56480C3DE5152 **SHA256:** 87C47D0E2E511DE24F20573FD90202DDCBB0C626118129769122FA870B8DF61A	text
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\pa\messages.json **MD5:** 97F769F51B83D35C260D1F8CFD7990AF **SHA256:** BBD37D41B7DE6F93948FA2437A7699D4C30A3C39E736179702F212CB36A3133C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old~RF10d5b1.TMP **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_metadata\verified_contents.json **MD5:** 8F99E1EF2AFC5F73D9391C248A0390AA **SHA256:** D57215628AF1ECD1ECD8F83DA69245161E4E0A2CE24846B2FFF6B35DA232709B	text
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\be\messages.json **MD5:** 68884DFDA320B85F9FC5244C2DD00568 **SHA256:** DDF16859A15F3EB3334D6241975CA3988AC3EAFC3D96452AC3A4AFD3644C8550	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\kk\messages.json **MD5:** 2D94A58795F7B1E6E43C9656A147AD3C **SHA256:** 548DC6C96E31A16CE355DC55C64833B08EF3FBA8BF33149031B4A685959E3AF4	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\ca\messages.json **MD5:** FBB841A2982166239D68907361F41F61 **SHA256:** DE6D7B7C2427EC4E738407D7834B71941F69166B030355E00F325FF1391DF5A1	binary

PID	Process	Filename	Type
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\th\messages.json **MD5:** 0875B0BAD81161CCF2C16E13EE49AF9D **SHA256:** D299AA0C4F29C5C8248A1C51AFDB7439F4CF7BC28EE02408A598F8AAD9F70810	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ar\messages.json **MD5:** 3EC93EA8F8422FDA079F8E5B3F386A73 **SHA256:** ABD0919121956AB535E6A235DE67764F46CFC944071FCF2302148F5FB0E8C65A	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\mn\messages.json **MD5:** 83E7A14B7FC60D4C66BF313C8A2BEF0B **SHA256:** 613D8751F6CC9D3FA319F4B7EA8B2BD3BED37FD077482CA825929DD7C12A69A8	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139\offscreendocument.html **MD5:** B747B5922A0BC74BBF0A9BC59DF7685F **SHA256:** B9FA2D52A4FFABB438B56184131B893B04655B01F336066415D4FE839EFE64E7	html
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139\128.png **MD5:** D056CEC3B05D6A863DDFA7EE4C1C9F0C **SHA256:** FF702CA753A7E3B75F9D9850CC9343E28E8D60F8005A2C955C8AC2105532B2C9	image
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\pl\messages.json **MD5:** 10BA7FE4CAB38642419BE8FEF9E78178 **SHA256:** 6538F562BD1BAA828C0EF0ADC5F7C96B4A0EB7814E6B9A2B585E4D3B92B0E61D	binary
8452	msedge.exe	C:\Users\admin\Downloads\smartonestartpdf.msi:Zone.Identifier **MD5:** FBCCF14D504B7B2DBCB5A5BDA75BD93B **SHA256:** EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913	text
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\am\messages.json **MD5:** 83E0E58D0752FF7C3F888E6406413B84 **SHA256:** 64E01BC292BA2EA1699576FCC445367047520EE895E290CCEE20C24C9336D8EF	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\bg\messages.json **MD5:** 2E6423F38E148AC5A5A041B1D5989CC0 **SHA256:** AC4A8B5B7C0B0DD1C07910F30DCFBDF1BCB701CFCFD182B6153FD3911D566C0E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\0a81f971-0f82-48d6-ad0f-0a731cabd9ea.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
8532	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139_locales\vi\messages.json **MD5:** 1E54AFBACCA335BE3A050920DDFBE863 **SHA256:** F1DA95E1D58E933050CD8A4FEA12F3D1B9A2759479FFDB74FDC1CFBF89568327	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1154777139\manifest.fingerprint **MD5:** 960A6760446FEDA24DB425BDB4123F21 **SHA256:** 7E69ED2C93D3A4CF2565D2712188A291A8A73470A1792039E760E01C174545D6	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\af\messages.json **MD5:** 12403EBCCE3AE8287A9E823C0256D205 **SHA256:** B40BDE5B612CFFF936370B32FB0C58CC205FC89937729504C6C0B527B60E2CBA	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ca\messages.json **MD5:** D177261FFE5F8AB4B3796D26835F8331 **SHA256:** D6E65238187A430FF29D4C10CF1C46B3F0FA4B91A5900A17C5DFD16E67FFC9BD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\de\messages.json **MD5:** D116453277CC860D196887CEC6432FFE **SHA256:** 36AC525FA6E28F18572D71D75293970E0E1EAD68F358C20DA4FDC643EEA2C1C5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\da\messages.json **MD5:** B922F7FD0E8CCAC31B411FC26542C5BA **SHA256:** 48847D57C75AF51A44CBF8F7EF1A4496C2007E58ED56D340724FDA1604FF9195	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\cs\messages.json **MD5:** CCB00C63E4814F7C46B06E4A142F2DE9 **SHA256:** 21AE66CE537095408D21670585AD12599B0F575FF2CB3EE34E3A48F8CC71CFAB	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\am\messages.json **MD5:** 9721EBCE89EC51EB2BAEB4159E2E4D8C **SHA256:** 3D0361A85ADFCD35D0DE74135723A75B646965E775188F7DCDD35E3E42DB788E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL\128.png **MD5:** 35696ABA596D5B8619A558DD05B4AD40 **SHA256:** 75DA533888189D13FC340D40637B9FC07A3F732E3FCF33EC300F4C7268790A62	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\el\messages.json **MD5:** 9ABA4337C670C6349BA38FDDC27C2106 **SHA256:** 37CA6AB271D6E7C9B00B846FDB969811C9CE7864A85B5714027050795EA24F00	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\bn\messages.json **MD5:** 651375C6AF22E2BCD228347A45E3C2C9 **SHA256:** 1DBF38E425C5C7FC39E8077A837DF0443692463BA1FBE94E288AB5A93242C46E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\az\messages.json **MD5:** 9A798FD298008074E59ECC253E2F2933 **SHA256:** 628145F4281FA825D75F1E332998904466ABD050E8B0DC8BB9B6A20488D78A66	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\en_CA\messages.json **MD5:** 07FFBE5F24CA348723FF8C6C488ABFB8 **SHA256:** 6895648577286002F1DC9C3366F558484EB7020D52BBF64A296406E61D09599C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\en_GB\messages.json **MD5:** 3734D498FB377CF5E4E2508B8131C0FA **SHA256:** AB5CDA04013DCE0195E80AF714FBF3A67675283768FFD062CF3CF16EDB49F5D4	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\es\messages.json **MD5:** F61916A206AC0E971CDCB63B29E580E3 **SHA256:** 2008F4FAAB71AB8C76A5D8811AD40102C380B6B929CE0BCE9C378A7CADFC05EB	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\en\messages.json **MD5:** 07FFBE5F24CA348723FF8C6C488ABFB8 **SHA256:** 6895648577286002F1DC9C3366F558484EB7020D52BBF64A296406E61D09599C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\en_US\messages.json **MD5:** 578215FBB8C12CB7E6CD73FBD16EC994 **SHA256:** 102B586B197EA7D6EDFEB874B97F95B05D229EA6A92780EA8544C4FF1E6BC5B1	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\es_419\messages.json **MD5:** 535331F8FB98894877811B14994FEA9D **SHA256:** 90A560FF82605DB7EDA26C90331650FF9E42C0B596CEDB79B23598DEC1B4988F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\et\messages.json **MD5:** 64204786E7A7C1ED9C241F1C59B81007 **SHA256:** CC31B877238DA6C1D51D9A6155FDE565727A1956572F466C387B7E41C4923A29	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\fil\messages.json **MD5:** FCEA43D62605860FFF41BE26BAD80169 **SHA256:** F51EEB7AAF5F2103C1043D520E5A4DE0FA75E4DC375E23A2C2C4AFD4D9293A72	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\fi\messages.json **MD5:** B38CBD6C2C5BFAA6EE252D573A0B12A1 **SHA256:** 2D752A5DBE80E34EA9A18C958B4C754F3BC10D63279484E4DF5880B8FD1894D2	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\gl\messages.json **MD5:** 6BAAFEE2F718BEFBC7CD58A04CCC6C92 **SHA256:** 0CF098DFE5BBB46FC0132B3CF0C54B06B4D2C8390D847EE2A65D20F9B7480F4C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\hu\messages.json **MD5:** 8930A51E3ACE3DD897C9E61A2AEA1D02 **SHA256:** 958C0F664FCA20855FA84293566B2DDB7F297185619143457D6479E6AC81D240	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\it\messages.json **MD5:** 0D82B734EF045D5FE7AA680B6A12E711 **SHA256:** F41862665B13C0B4C4F562EF1743684CCE29D4BCF7FE3EA494208DF253E33885	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\lv\messages.json **MD5:** A568A58817375590007D1B8ABCAEBF82 **SHA256:** 0621DE9161748F45D53052ED8A430962139D7F19074C7FFE7223ECB06B0B87DB	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\fr_CA\messages.json **MD5:** 6CAC04BDCC09034981B4AB567B00C296 **SHA256:** 4CAA46656ECC46A420AA98D3307731E84F5AC1A89111D2E808A228C436D83834	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\fr\messages.json **MD5:** A58C0EEBD5DC6BB5D91DAF923BD3A2AA **SHA256:** 0518287950A8B010FFC8D52554EB82E5D93B6C3571823B7CECA898906C11ABCC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\gu\messages.json **MD5:** BC7E1D09028B085B74CB4E04D8A90814 **SHA256:** FE8218DF25DB54E633927C4A1640B1A41B8E6CB3360FA386B5382F833B0B237C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\hr\messages.json **MD5:** 25CDFF9D60C5FC4740A48EF9804BF5C7 **SHA256:** 73E6E246CEEAB9875625CD4889FBF931F93B7B9DEAA11288AE1A0F8A6E311E76	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\id\messages.json **MD5:** 34D6EE258AF9429465AE6A078C2FB1F5 **SHA256:** E3C86DDD2EFEBE88EED8484765A9868202546149753E03A61EB7C28FD62CFCA1	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\fa\messages.json **MD5:** 097F3BA8DE41A0AAF436C783DCFE7EF3 **SHA256:** 7C4C09D19AC4DA30CC0F7F521825F44C4DFBC19482A127FBFB2B74B3468F48F1	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ja\messages.json **MD5:** 15EC1963FC113D4AD6E7E59AE5DE7C0A **SHA256:** 34AC08F3C4F2D42962A3395508818B48CA323D22F498738CC9F09E78CB197D73	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\mr\messages.json **MD5:** 3B98C4ED8874A160C3789FEAD5553CFA **SHA256:** ADEB082A9C754DFD5A9D47340A3DDCC19BF9C7EFA6E629A2F1796305F1C9A66F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ko\messages.json **MD5:** F3E59EEEB007144EA26306C20E04C292 **SHA256:** C52D9B955D229373725A6E713334BBB31EA72EFA9B5CF4FBD76A566417B12CAC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ml\messages.json **MD5:** 4717EFE4651F94EFF6ACB6653E868D1A **SHA256:** 22CA9415E294D9C3EC3384B9D08CDAF5164AF73B4E4C251559E09E529C843EA6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\sk\messages.json **MD5:** 8E55817BF7A87052F11FE554A61C52D5 **SHA256:** 903060EC9E76040B46DEB47BBB041D0B28A6816CB9B892D7342FC7DC6782F87C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\sv\messages.json **MD5:** 90D8FB448CE9C0B9BA3D07FB8DE6D7EE **SHA256:** 64B1E422B346AB77C5D1C77142685B3FF7661D498767D104B0C24CB36D0EB859	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ne\messages.json **MD5:** B1083DA5EC718D1F2F093BD3D1FB4F37 **SHA256:** E6ED0A023EF31705CCCBAF1E07F2B4B2279059296B5CA973D2070417BA16F790	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\nl\messages.json **MD5:** 32DF72F14BE59A9BC9777113A8B21DE6 **SHA256:** F3FE1FFCB182183B76E1B46C4463168C746A38E461FD25CA91FF2A40846F1D61	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\pt_BR\messages.json **MD5:** 608551F7026E6BA8C0CF85D9AC11F8E3 **SHA256:** A73EEA087164620FA2260D3910D3FBE302ED85F454EDB1493A4F287D42FC882F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\no\messages.json **MD5:** A1744B0F53CCF889955B95108367F9C8 **SHA256:** 21CEFF02B45A4BFD60D144879DFA9F427949A027DD49A3EB0E9E345BD0B7C9A8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\lt\messages.json **MD5:** 970544AB4622701FFDF66DC556847652 **SHA256:** 5DFCBD4DFEAEC3ABE973A78277D3BD02CD77AE635D5C8CD1F816446C61808F59	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\pl\messages.json **MD5:** B8D55E4E3B9619784AECA61BA15C9C0F **SHA256:** E00FF20437599A5C184CA0C79546CB6500171A95E5F24B9B5535E89A89D3EC3D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ro\messages.json **MD5:** BED8332AB788098D276B448EC2B33351 **SHA256:** 085787999D78FADFF9600C9DC5E3FF4FB4EB9BE06D6BB19DF2EEF8C284BE7B20	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\hi\messages.json **MD5:** 98A7FC3E2E05AFFFC1CFE4A029F47476 **SHA256:** D2D1AFA224CDA388FF1DC8FAC24CDA228D7CE09DE5D375947D7207FA4A6C4F8D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\kn\messages.json **MD5:** 38BE0974108FC1CC30F13D8230EE5C40 **SHA256:** 30078EF35A76E02A400F03B3698708A0145D9B57241CC4009E010696895CF3A1	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\pt_PT\messages.json **MD5:** 0963F2F3641A62A78B02825F6FA3941C **SHA256:** E93B8E7FB86D2F7DFAE57416BB1FB6EE0EEA25629B972A5922940F0023C85F90	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ms\messages.json **MD5:** 7D273824B1E22426C033FF5D8D7162B7 **SHA256:** 2824CF97513DC3ECC261F378BFD595AE95A5997E9D1C63F5731A58B1F8CD54F9	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\tr\messages.json **MD5:** 76B59AAACC7B469792694CF3855D3F4C **SHA256:** B9066A162BEE00FD50DC48C71B32B69DFFA362A01F84B45698B017A624F46824	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ru\messages.json **MD5:** 51D34FE303D0C90EE409A2397FCA437D **SHA256:** BE733625ACD03158103D62BC0EEF272CA3F265AC30C87A6A03467481A177DAE3	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ta\messages.json **MD5:** DCC0D1725AEAEAAF1690EF8053529601 **SHA256:** 6282BF9DF12AD453858B0B531C8999D5FD6251EB855234546A1B30858462231A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\th\messages.json **MD5:** 64077E3D186E585A8BEA86FF415AA19D **SHA256:** D147631B2334A25B8AA4519E4A30FB3A1A85B6A0396BC688C68DC124EC387D58	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\uk\messages.json **MD5:** 970963C25C2CEF16BB6F60952E103105 **SHA256:** 9FA26FF09F6ACDE2457ED366C0C4124B6CAC1435D0C4FD8A870A0C090417DA19	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\te\messages.json **MD5:** 385E65EF723F1C4018EEE6E4E56BC03F **SHA256:** 026C164BAE27DBB36A564888A796AA3F188AAD9E0C37176D48910395CF772CEA	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\sw\messages.json **MD5:** D0579209686889E079D87C23817EDDD5 **SHA256:** 0D20680B74AF10EF8C754FCDE259124A438DCE3848305B0CAF994D98E787D263	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\sl\messages.json **MD5:** BFAEFEFF32813DF91C56B71B79EC2AF4 **SHA256:** AAB9CF9098294A46DC0F2FA468AFFF7CA7C323A1A0EFA70C9DB1E3A4DA05D1D4	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\sr\messages.json **MD5:** 7F5F8933D2D078618496C67526A2B066 **SHA256:** 4E8B69E864F57CDDD4DC4E4FAF2C28D496874D06016BC22E8D39E0CB69552769	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\vi\messages.json **MD5:** 773A3B9E708D052D6CBAA6D55C8A5438 **SHA256:** 597C5F32BC999746BC5C2ED1E5115C523B7EB1D33F81B042203E1C1DF4BBCAFE	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\zh_CN\messages.json **MD5:** 3E76788E17E62FB49FB5ED5F4E7A3DCE **SHA256:** E72D0BB08CC3005556E95A498BD737E7783BB0E56DCC202E7D27A536616F5EE0	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\ur\messages.json **MD5:** 8B4DF6A9281333341C939C244DDB7648 **SHA256:** 5DA836224D0F3A96F1C5EB5063061AAD837CA9FC6FED15D19C66DA25CF56F8AC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Rules\LOG.old **MD5:** E30B48D8AE2479EF529F0AB65CB1F975 **SHA256:** DEE4176B1D6450A9A96383F5007E77C4C7D8CD43115F5953C139926D20C9591E	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Scripts\LOG.old~RF10d8fd.TMP **MD5:** 61A40A6640E8F12CB329C1E36223E2C9 **SHA256:** B311101250AAE9917310821EFCB0D9E43FC4B29AA2BE0E6C8CF066DA8FA730D9	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Rules\LOG.old~RF10d8fd.TMP **MD5:** 8FFDD5580E3C319A0F8610CF97BBD782 **SHA256:** 8391517B70D41DA3CBE3E1E51E275A3DE6514C8F9DA5C4BA2F0BD1859BCB0106	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir3956_1322702627\CRX_INSTALL_locales\zh_TW\messages.json **MD5:** 0E60627ACFD18F44D4DF469D8DCE6D30 **SHA256:** F94C6DDEDF067642A1AF18D629778EC65E02B6097A8532B7E794502747AEB008	binary
9004	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi\d8b759c1-a68e-43e4-ac76-eee9e4ad4410.down_data **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Scripts\LOG.old **MD5:** D392F4191F0DFF78511FBDE7E3E08BF6 **SHA256:** 2AEA14504BC6FD1BD5869775B27795446DE98AED4A5C8D8D467E2F542F935A5E	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF10da64.TMP **MD5:** 86A581376460D1DE379EA1CDE245C48A **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\7180c59a-e43d-4ac3-95ac-75ff09d1fce8.tmp **MD5:** 7E8EFAB591A7794E224ADC063AB89622 **SHA256:** 59015A92ED553AD9EDD4F7C618DCD5751462C996E6016BD6DC811E5B55BE1091	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\928a9c7d-6675-4d5c-86a9-8a8868b6af0a.tmp **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries~RF10e0ad.TMP **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF10d9e7.TMP	binary

PID	Process	Filename	Type
		MD5: 21F2F7C19D1307E226AA9B173699668F **SHA256:** EBA4881D0D52E08E8D6899BFFC1AB4F59798E9C70D1C2F51875E78D8BAA11C2A	
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity **MD5:** 7E8EFAB591A7794E224ADC063AB89622 **SHA256:** 59015A92ED553AD9EDD4F7C618DCD5751462C996E6016BD6DC811E5B55BE1091	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\aac028c8-259e-4028-82e4-f32dd86de509.tmp **MD5:** 9A6905288E617971C3AB798DDEA78800 **SHA256:** BDFD75375045EFE0DA79655AC4AE9623DF229571EDFF6CCC8DEB9657BE15C564	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RF10e0ad.TMP **MD5:** FDF62CB6FD1CDDE50143B56A62355BF1 **SHA256:** 1F2755713752AB9B63A512BF29F2B3798F2C5372AF699EDCC6C7F72D457C9A7E	binary
3956	msedge.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content \FE17BEC2A573BC9AE36869D0274FFA19_6DA81F04C5F9EAD2CD0268808FCE61E1 **MD5:** 7E5E9912DE7A985FF6257B5E3005DE2C **SHA256:** EC0BDEA0FCC54BE0A302CAC5A2513186CCD5A9E1BD9DE7C8DD81CE1773141571	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences **MD5:** B40C71321A808309292DEB4485184B08 **SHA256:** A7DA464FA5EAEAA9DDFF7BA3CCE48C6483CE9738F22F7D87BFF373318DF5C28F	binary
3956	msedge.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData \248DDD9FCF61002E219645695E3FFC98_047665DA31D3B6D49BCD9D6BF2556F80 **MD5:** A2BD61F30DC47B36DC3F9DE6A1BE11D7 **SHA256:** 89F274A5A39B105DEB464C8E49FDD05CB742DD91E36DC8040E1D546ADB7311A8	binary
3956	msedge.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData \FE17BEC2A573BC9AE36869D0274FFA19_6DA81F04C5F9EAD2CD0268808FCE61E1 **MD5:** 0D00A1CDECFFB1493D3C4E2B2260EE28 **SHA256:** 83665ED989DBF4EB9DC521E6F93FF94B75F5A8E0F76C28D38FBF584634837508	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\dae51727-acdc-471d-b65e-a2e728c66ca3.tmp **MD5:** B40C71321A808309292DEB4485184B08 **SHA256:** A7DA464FA5EAEAA9DDFF7BA3CCE48C6483CE9738F22F7D87BFF373318DF5C28F	binary
3956	msedge.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content \248DDD9FCF61002E219645695E3FFC98_047665DA31D3B6D49BCD9D6BF2556F80 **MD5:** 83B36047F1DDA57B944E63707D852A2A **SHA256:** F0C224954428A04411AACF749CAFCEC36E80507E81701AC810BC7739032EB9CB	binary
9004	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\Microsoft\CryptnetUrlCache \Content\26C212D9399727259664BDFCA073966E_F9F7D6A7ECE73106D2A8C63168CDA10D **MD5:** 38989CDC9B939CBF439472EC8FEBE5D7 **SHA256:** 05491F06DCD3C4FBB8FF3B2D2007CD4DFE1CE2B651587DF866B2657984EFB329	binary
9004	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi \d8b759c1-a68e-43e4-ac76-eee9e4ad4410.9c653a74-9b7f-49e8-a351-18e6aa9aa109.down_meta **MD5:** 02FEEC0B5368D0F03B6C10A2DD33F7B2 **SHA256:** —	binary
9004	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\Microsoft\CryptnetUrlCache \MetaData\26C212D9399727259664BDFCA073966E_F9F7D6A7ECE73106D2A8C63168CDA10D **MD5:** BDEE581ED34F29CA8DCD99896CFCD71A **SHA256:** DF12F92B4CD8F19CDB7789D8FA9C9D81A8FA6443650322AFD035DBBAFFCD5732	binary
9004	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi \37aca0a8-4812-4c33-91dd-492195ea7795.up_meta_secure **MD5:** 789146C48EE621E0C660EFE8E112A581 **SHA256:** 74268007D77DE496BDFDA54C892F01156341F5090054ADEE171EBDEBBD3FFA23	binary
9004	BackgroundTransferHost.exe	C:\Users\admin\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\AC\BackgroundTransferApi \37aca0a8-4812-4c33-91dd-492195ea7795.9c653a74-9b7f-49e8-a351-18e6aa9aa109.down_meta **MD5:** 02FEEC0B5368D0F03B6C10A2DD33F7B2 **SHA256:** 4E20FEDC453B6F84F282B4C3B3EF113B97D6481EBEB0503513D7CBD8E381FF90	binary
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSIF34C.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSIF232.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSIF429.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSIF498.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSIF449.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSIF408.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSIF4F8.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Secure Preferences **MD5:** 31F912FB938EE6F3AC4EA90BB480FE1B **SHA256:** 56317D81592EA57FE2EA12458CBAE40114792482B769DF2B4E8E299D23964877	binary
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSIF4B8.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index~RF11150c.TMP **MD5:** 01F0B29822F7C00694ABF3150276196A **SHA256:** C5CA04147E678498F16E8DED9EFB227591ABF40A3AFC5E65248D019D9B9198D9	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Secure Preferences~RF10f4a3.TMP **MD5:** 9BC4DCC68994EB09A084CC44ECC6F4E6 **SHA256:** 2D81681CA8E90F7F0FC48382D8AF4336F937EEB1FB49ACFD5249584502D86143	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF110423.TMP **MD5:** 9A6905288E617971C3AB798DDEA78800 **SHA256:** BDFD75375045EFE0DA79655AC4AE9623DF229571EDFF6CCC8DEB9657BE15C564	binary
8100	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG **MD5:** 8EAF164D9AF3FFA9C8ED62BADCA7EC07 **SHA256:** E3A5D1676B9D6C75E79EF00C6F18DF9B21589A8593F840DFDA0A33B67E2534D2	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\7bc4b9be-0e6f-4f42-8765-9bad7d3c680a.tmp **MD5:** 31F912FB938EE6F3AC4EA90BB480FE1B **SHA256:** 56317D81592EA57FE2EA12458CBAE40114792482B769DF2B4E8E299D23964877	binary
8100	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\000003.log **MD5:** 1B6AE383CD94AF67CB20942365975A8D **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\87015544-8b0a-409f-b693-7be157375ca2.tmp **MD5:** 78BB216E06E8ACCCE662159FC222F6A4 **SHA256:** B287F620836469CE59FF80699F4EA19A783BF91A1967D8A3E824F3F959BE926A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF110423.TMP **MD5:** B40C71321A808309292DEB4485184B08 **SHA256:** A7DA464FA5EAEAA9DDFF7BA3CCE48C6483CE9738F22F7D87BFF373318DF5C28F	binary
664	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG **MD5:** 15F0BFB0D949E25F4128F2B240F3446D **SHA256:** C6E674A93F5BACCBB25BF80BE2ADD4D953DE1DB30A2F559C82381880F4927682	text
664	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\000013.log **MD5:** E12F86D62C04479EFDD9D9BA360A40A1 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\3f481e1e-9d5b-4fd3-88b9-e63bf05bba7f.tmp **MD5:** 78B57F0875E826BA0BDE7851DC60EB7F **SHA256:** 921693D034420C3AA9CD228C79ED4023A59C9383902A4D389C0E3DE614F31674	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\7af97ceb8d4ea843_0 **MD5:** EEF9DFFBAA8996C03B0DB9AC6BD59D27 **SHA256:** 9C4B6B267509B083C532C4EECF3FC4346B3A845C1DF8B65543C94779AB00AE19	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\14858ffe899bd6d1_0 **MD5:** 8E029A8559C3D7FD9A85122DD8E2E4C2 **SHA256:** 37605418DC5E8E48E502AB52A6058A5160FC84625BCA7A6B11ADBACDF6D7536E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\e2c3a160-4f93-438f-98b9-c43dc53195cf.tmp **MD5:** E1176CA688A2F72CBD1F60A5D075A706 **SHA256:** 589BCE0F7B8DC7F1A3451BD891251E7945B599C03473182F5040DF31FD2DA184	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000268 **MD5:** 4FCE397499B357E61A483A348FC3CCE5 **SHA256:** 9FFE4BF959D23AB768D6DF385C5AE11F8697FA0610C5D5EE5B06862F4F0E0B11	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\d2db12924f4c186a_0 **MD5:** 89EACCFCA43BC3990B417B8543C8B9D4 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\fc33723c1bc2cc07_0 **MD5:** F907D1723FD2B45F6E7F1B9E5F1851C6 **SHA256:** A122C861139FEB3264DA2DF0C94D7D00AB4010C7690E0DFA173A7A000AAE73E6	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000269 **MD5:** 5B1D56A382E9FB96FA1D82EB429B9664 **SHA256:** 8861F7F4F9F273B5AD1FD18B73ECD0F8A19111A950DAAD8C34DE0EE34AF9F1FD	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00026a **MD5:** AC9E9A0D7296DF43FDF0F61B8176869B **SHA256:** D62033CB360828BC42885E3838B36C99F070D0462E6E75BFF4626CFA00E6A6CB	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF114f36.TMP **MD5:** 78B57F0875E826BA0BDE7851DC60EB7F **SHA256:** 921693D034420C3AA9CD228C79ED4023A59C9383902A4D389C0E3DE614F31674	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\fa6905cce0db35d4_0 **MD5:** A42EF9EC3C4B280835D5C369F759D712 **SHA256:** 6A00BE6F6EAB5AA8B4D6899A47D454F49ABD72E0E258387DDDEA70C8342708A5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\5c9e62de0948215d_0 **MD5:** 52D6D56C4EF07B88C36CB60CFF15382F **SHA256:** A19A33E09436B427381485C8208948AF7D7DBFB9D0E7377479087AB852A0C4F0	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00026b **MD5:** BA4558901922434B04B1AB9035C7716C **SHA256:** 8BE74600DF523851845BBD3FA288F7B7E65C7C8BFC8B9148783EBEE3ACFB05CE	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00026c **MD5:** 4A68983965BB0EE2328181E4AF6DA7CC **SHA256:** A999576CDB4DE9CB0010A1B626595F9EE94F10206F088103253AD0273F1A30C8	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\75e88d68b23defff_0 **MD5:** 91C9DFC9D62EE9EA1919EB6E359C2B2F **SHA256:** 2735D21D99CDF9576F5BCB0A9F132263796C1E3CB61EA85EE96BB7C4212BE847	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\077e930417a8eb0a_0 **MD5:** AE3CE2C5577CDF05CA94C695C56D0D75 **SHA256:** 5C5509E064AC9CE037B1A85F181405B3E21B7409AC70A037ED5B50EE128E41B1	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00026d **MD5:** C7A98E859C16A982F15A697C5EF2C9FF **SHA256:** 04F334C818EC55942124F51F18F341C616DE8494933256CEE0C7F98FA5FD8AFE	compressed
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\a64776383623fc80_0 **MD5:** 71748684DF2EBA5EF38AB43F8C84BCBD **SHA256:** 68D11385FFEFB0E0FD0816CB4DD8D242B31586A1904501797D52A7D95D769984	binary

PID	Process	Filename	Type
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00026e **MD5:** 91B2E1E1B5E4372DE739ACA27EDFC8E9 **SHA256:** 0E91DE3B69C5888257CF73C62DC80B611BB1861829E0BA73C031AA3020EA8524	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00026f **MD5:** 7AD992EC24D2F4B93A3673BDFE2177C1 **SHA256:** FB76559867F9DC8EDF38FC5FAABBE9AC140DFC27E6C1A727BAE9BC184F134EC6	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000271 **MD5:** 7CEBDF652E35654DA35F24CB1772C2EC **SHA256:** 593EF957F43A1D66D2ADB377D8DCCE016EC0329DF93AC0A4214BD02C0C28128B	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000270 **MD5:** 635FCD978BE7BCEBAD54647D94C00073 **SHA256:** 65D1009E1C530091A26F2862BCB419EDDB32B3850E2D4839CC84CC8C908A47EB	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\4c54f31bb706c996_0 **MD5:** 49F7553A835424C94F7250838FEC33A7 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\19efb25a29610664_0 **MD5:** 5E79E4B51671254B4D77E600129EC06D **SHA256:** CB5157A34BBAE73166A78869F7BF6E66459A8614BA21AF8CA6153737AE68A933	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\99aad9685e0b4e3f_0 **MD5:** 3E6F9B136E057C7082FBCF72141A7EFC **SHA256:** EC71E07680610CBF7B384B3B566B470F1E99F3510BBD88BE59131A50E7B7C412	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\5f45fbd79d51d247_0 **MD5:** C924C182552252A3C36ACAA0516BD190 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\3e83648d7c572086_0 **MD5:** 5B79D9E2772222F526847A9574ECFA4A **SHA256:** E91140F5E793C429006B2051630F87E57CA106783CD865E37A454AD016E10B3C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\c336290655f9659d_0 **MD5:** 87C55EEB9E5A870BD9920700E3CFE7BC **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\e5d0a5e755bacf68_0 **MD5:** 06FFC71D51197640D3F68526A86A2211 **SHA256:** B8CC3A965DF5EBBE3F0F3B8C561EFE2DA117F2753A725C1140E970E298630791	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000275 **MD5:** 799EF9B8727E6FC3FD73A849FF2879D1 **SHA256:** 11F4BB0D1D713E517D5BE48DDE8FDB3059D9887F5A6B84AD9D2D31C1858B1089	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000273 **MD5:** BDA2EEF61BE686F3BF7C3C453AF5ECEE **SHA256:** F1AAAF95A0BF490838DFE1E6F27EDBD9868EE78620FDE23DE13908A273E0FC80	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\432b256a7cc84e8d_0 **MD5:** CD8F2BD480D1C5D2A07AD7268880B024 **SHA256:** 71002AF52882802605D33BCBC6053B0E9A4CC772E770622616A956E4843DCB55	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000274 **MD5:** 1E7F10E4707261A3A2B8311C9CC53F79 **SHA256:** 3969C4B58B1DAFDBFE8080DEEE2BDA551BE5910821845668986A77D97FC63267	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000276 **MD5:** 992AF40CE4E30A3F93F14D074C7008D4 **SHA256:** 2350023A9682197C2E9E20D2AF3A1A9A5D58AC583E8434892CE1A16877C3B8F1	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\09342914efa5cb9e_0 **MD5:** 3B39B8A8C6131197490672D43A189D9A **SHA256:** 5C8DEEB9D6131AF93CAD96A94D85446D1E506F9D832279BEFF14273F4B68B131	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\ad270e96489e5285_0 **MD5:** EE781A188986BA8ED5D11EE0A6E16410 **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000272 **MD5:** 1F07DAAA54F5889BC3639D19F6AF57BD **SHA256:** 61DA1F0D532A5D422BC70E9275293C26898A749C169FFCFE57D5B44BF765C33A	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\f431509c98696541_0 **MD5:** FECD531BF99C773E3DA2B59526458F77 **SHA256:** 8BFFA60158F418ED0217C1F5DFCDB16833E77FF01666107E01B9C1D69AA54E60	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\3866c965c8eee998_0 **MD5:** E48DC50AF5693C7A5EC237B959A55C35 **SHA256:** 6E184863EEC2A340E4F112B7A1A0FFD532AAF51274E498EFA062A6D3BBAF8074	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\5f34c475642fe211_0 **MD5:** E761D94A6F280CC35118DEF41A8886B6 **SHA256:** BA5069926F4066DB0BD5CC3281DCCA3D40035E9DF75F6D7ED252CD058A2B8698	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000277 **MD5:** 7596FF2A22264DC1A0832933D91F4E0C **SHA256:** 052D23806E10C7F316B28B4D4DA04DE57A908EC8418F259FFEF9A2116AD2D175	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\75836a7e13de64f6_0 **MD5:** 5A33A8318D71B4C67F036B5A522031C4 **SHA256:** A2214DB0A08E2DD116397C201940F2187B02FA7B3B489982E27DD5BB4C229E3B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\1760ab97345a0135_0 **MD5:** 1865AB8992489B339D63538DC346A6A1 **SHA256:** 95CE3B9636488E729B3B06E2B0F0B3AB9E81E764457C5D682C132F47A94D0B1E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\8fc7378fc21349c0_0 **MD5:** 8524F4444266726193D7E0E92BD06B3A **SHA256:** BAC57E573069E09D82BCAEC16F031A17F2D29F3524F7457A3AB28DD114755285	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000279 **MD5:** DA52215788713F65C04B1D02F6F7AB37 **SHA256:** 2C1DFFA386C7D9B1EF8F331B7DE9F7D990F38C4860FC26F319F7692D085DC65D	image

PID	Process	Filename	Type
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000278 **MD5:** CD4E35DA59C27AC7A5C33EE6338F7984 **SHA256:** AD611F1A5A2EBB0C347E1A6144F3188B452F20AEF2A9BC3914C522EA9BA8ED32	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00027a **MD5:** 6BB24C9D9FF58ACBDDAD794AD503BF81 **SHA256:** C8D218245772C237B06F0A821D33DB7CAA56504CD70C172970372189EB7A9201	compressed
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00027b **MD5:** FFE32C33B16B090A803956BC7DEFE605 **SHA256:** B1604E6C823BFD5B3B1313CF52B387A4908E7283FC90765474A99D5B33FA6D2A	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00027c **MD5:** 54A8931FD95DB7FC7C0E87E89D8CCB4B **SHA256:** —	compressed
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\b329cae80b8e3759_0 **MD5:** EB997ED50DC0EFD3A8F194ADE26AC153 **SHA256:** FFFD6352C04E5CF84DE5E928FE7C61D0793AA7B0900B4D5C473A230BF1B188F4	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00027e **MD5:** 199F0B7DD376B35AA28ADD76787A8C74 **SHA256:** DBBB41988C967372C8AF20C6FA086CDE8E5B2055B0D1D82C31D6464915A4D77A	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00027f **MD5:** E6F8F9147A0BE7B69ED7723DD06C4C02 **SHA256:** 466C7B462274F9206BE41534E27AE9548E019A8F2CD5D72492B5ACE01B272E55	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000281 **MD5:** 40919B50042D502ED70915F428E537C3 **SHA256:** D5B2E433B922C188FA2EB66B62D9031FEAA8BE56E7991C55F012869685921980	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\index.txt.tmp **MD5:** 9361AA56349F45C5EDB4C5C356B39365 **SHA256:** A8048C5F8BAD444B647462A5C843B38FE5CF69057015B4B00A4FE3713D45784F	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000280 **MD5:** 6793FA249DD0A792D9DCBBFF58116244 **SHA256:** 04ACFF19EB7DABE3DAEA20E107798E785B84F8BD57D8457C75FF2E587C392BEB	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\d85a540a786e2b75_0 **MD5:** C45D5CFAA8FC432AFC6A7681588F0661 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\index.txt **MD5:** 9361AA56349F45C5EDB4C5C356B39365 **SHA256:** A8048C5F8BAD444B647462A5C843B38FE5CF69057015B4B00A4FE3713D45784F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\index.txt~RF115ab0.TMP **MD5:** DC73B73D50D53D846488C30ABAE6D8E4 **SHA256:** 0F823D2ED58E4004A9B5C33FE0C4DC13BDEE758B79DB83180261A5AE22F9A34A	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00027d **MD5:** E3599B0C19DEF05340F242E6D6CD76CC **SHA256:** 350E8D47BAB4B1A76033D1EC6B302892595F17047BAC4E76581D1FE9E2BF7A61	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000284 **MD5:** 99967367316F76224F3176E560C0C95F **SHA256:** 860449D63FC7FF08B68040598F519A7326E8B431C50E9AB22E98E3D7B5E8DEFD	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000282 **MD5:** AA2CB1A2F49DA4E981FFA009A10C330A **SHA256:** 844EDA3EC4F029CE836DB805CB983833221FE6BA91D3B32EE13896541EE738FC	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\fd02545988169cfe_0 **MD5:** BF4492E9D2ED99305454CFB7978C34ED **SHA256:** 888B4678F62698FC275937C589A50E0AA9239A765FA45C89F95DC90EE6018D21	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000285 **MD5:** E16C3C51E4B5E5319D20DE9B6FA8F53E **SHA256:** 65B5E0EE574266DFA8291CF6CBD9DAD69186DABC379044C1A9431F5A2D6B0EE5	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\0a55d2702a5a973e_0 **MD5:** 880A170279251B5799A1E975404A2BFC **SHA256:** F7E605B952F5812D6D5051C4DB9AC1A39D819E8E532B062347257AA22DC3FCE9	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000283 **MD5:** C9D031E3E23EE5B946C8F94DB7DFD018 **SHA256:** 8B2F9AA7BEA182822815413C4CEF51F4161EFA40C429FC4F83308657F3F01993	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\421c34a7afb29e73_0 **MD5:** BD4E826519CB0ADC0934150EA88DCB9F **SHA256:** B94A9F7CB1BBA43D8E0E7E4E7ABBEF57ED78579F27A0AAD35FDFE1BBBC39698F	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000286 **MD5:** 2F5476BCBE988A55B715C4BEBD202909 **SHA256:** 8367090C865E689768D236AAAFB05BEFC67FC09C965D7EF967D373EE79D5646C	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\26e8641c9d788fe7_0 **MD5:** 0BEB82B7C2A3BF7FC1D2749249681AFD **SHA256:** CE1A9598A3B6D0C1F0DDD2242E33367CE6D6F6E0BAA1DD399BB1D46FC9129924	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\679e0b19c1929413_0 **MD5:** F58325289DCB8EE21D1B34335BFBF960 **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000287 **MD5:** 136D14A8239CF3A3DF327FDD4F4678C5 **SHA256:** C6BB62177BD54CACBC0C5CA21835C8808AD63B87BE314608E47BC2A1B4CAE402	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\f800ea87c4a769bd_0 **MD5:** 99CE81317859014C333F302CE6CFE31B **SHA256:** 4A74C416679F614FCA552C610C1094EB08FBA46A403ABDBAF51F8D1C16E18412	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\1e815ccad698a693_0	binary

PID	Process	Filename	Type
		MD5: D1D1042B4CABF14DF58C5FF267706903 **SHA256:** CF6F50816D6C0440C46951B794BDE26098FA7BBF7FD4E492A3DDDA4BF11564E5	
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\4371809e4892ce3a_0 **MD5:** 9D3BEC0C0A9B3B122B92FC5E32C2FA4A **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\ac0a639db1382d8f_0 **MD5:** D397E6911B9AFCB517F0FEFC286256AA **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\d97d87490ea93914_0 **MD5:** BFF3F29EB0863C8CFA8FC7A1F8C0703E **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000288 **MD5:** 238CBE5F258FF293FD0E4C1E1F3F3E9B **SHA256:** 325FFC739B248CA0B4161ED1FA46CCDE334B010267099331F00FAE22BF68B92F	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\29251a32ed36ed24_0 **MD5:** 93D5238E1B55A2D7BE4EC217AB46354B **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\831b748d813e87c1_0 **MD5:** 09F4A9438D2D90C17CB00D56099BBD59 **SHA256:** 4079D00D3E090023AAE23212AA5809F1526F9741C557AD0D7F3ED247D27F2D74	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\a09140056a5472d3_0 **MD5:** A2B3AC26B0CA769F44CF0F1CD26E88A3 **SHA256:** 1E4B0B04FB669C0C9F56F96EA4942B2A50A134F382908FB5B31EE7F596EAADB6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\70a92dd39e8a9706_0 **MD5:** 1761E5EB13D3905BF3BAC28FA6E521FC **SHA256:** C4074B90611D66568EFBAC23F87679C2E13D9AE9093D685E85866338DB9703A5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\d354de963313594a_0 **MD5:** DFFD7F9E3C286CDDC7D87D56EC2A61D0 **SHA256:** F2101499EB91F3FFD66672F60A2C1843664DFC545C3CDD1D8FFD229FF3C68F9F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\34005d8bbe63ac8f_0 **MD5:** 9291EDF5FD67A60D74A5B3958FC156E6 **SHA256:** E8A40B8B47C36020072CA37F8A8BCC63AC6BBB22D3B802250649223349E822C6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\1f42619cc72015b1_0 **MD5:** B1F8A2D2ADE011E705A8817364D3D5C5 **SHA256:** 317A5C73F1CECBDBD739C60DED73DD8DA7E5479D3FCB68888684DD58EB1CC19A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\8239969d23d64286_0 **MD5:** 2F40745C6847742975CA2E2D9269F30B **SHA256:** 0CFD7F15E32809DC836BB0EBF6B2F0898EA29C32DC8D8206C3EB02B6069FBA64	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\976832b43171a7dc_0 **MD5:** 7C0DF6E585BB70860AC070D52909321A **SHA256:** 0F639D75CE5B0A75F569AED9B16A6C20383363F4377B202B145C9209D0BF8187	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\af3c5977250ac262_0 **MD5:** CB8E03BEEC97F573622FCF5CEEAC562B **SHA256:** B4A1D2F76517001B951490503E1D789E3D781768ECD01F456BEC850322B270E8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\1fc9c6de2c4c64c6_0 **MD5:** F862580C3BA293E6AD4A4044F180F759 **SHA256:** 6D55E88EF15F5981D2C1306F56A22FC3C5EE06A2312B1280AE7255359ABD16A1	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\5aab1f47b4ff0085_0 **MD5:** D067ABE740D3BF90C600713CFB5A73CB **SHA256:** 1537ECACC28EBBD647AE6204C8659782AB00E312D714A40AB01B308A578A09E7	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\28a6e0e6c78b17e5_0 **MD5:** 945B6F90A59340ECB6A43F9D1BB54693 **SHA256:** 194FD1559A5996099D636913DF59A58309D682D28D8DF8813159454D3ABB9F2A	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000289 **MD5:** E8FD975434CB1F698F1E0173CAD1C460 **SHA256:** F91E409EDD3F9D9644956AE5C98364E1A848C3CDA320794A6BA06302601F5EEF	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00028a **MD5:** 40D80F164723BEDAA413CDF59DD08B66 **SHA256:** 1EC3DD468C2DDC82F8E1F79A29BD3250B5462108F659CF7AD0AD2B948D7AD8E0	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\08a67bdbc687e555_0 **MD5:** 096115C5F06E063F451E33084AD3A133 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\5e4a5380b773e295_0 **MD5:** 2BE91F3A6684FCDDC39894B41C8F09D5 **SHA256:** 8D47B5DCCE15381D81500F9423263660D98801028B22174047C69E78751590EB	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\4214239590ab25b0_0 **MD5:** D4737D0D760ED2FE646D5A75DA88F77E **SHA256:** D334B2807313FCD4FFFAEDD80FC862164C58FD2FAE8CA3B15812F9BB90166F69	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\f7359965305608c9_0 **MD5:** ED4BBB463C3B134B122BADCAC9B3556C **SHA256:** 95E2D77B3CD66C2AE37C63569E14CC4DD7F10C5F42096F3383D95F234E111BDB	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00028b **MD5:** CB864CFDAE5D53B4064FC7592794A416 **SHA256:** 34DE2763509BC15FC1918E2DA1D3D84F582CDBADFA2F804FBCFBE0DB25F30672	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\3b92aebc8164ab4c_0 **MD5:** 003874208103574A25E27E88601ECACD **SHA256:** 33677629F35A232D1053F38FF7D0D6526844CAE8D1A1F20FDFA55A44D79C99B4	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\7c024618eb0c8874_0 **MD5:** 2C4A47AF8AF1ED01CF8485B029AC0D60 **SHA256:** 1713B03F671862FA66022F62B7C19330F4B7E68B026B6701CDDD404BE69BC5D6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\ee3e297fc62b5c57_0	binary

PID	Process	Filename	Type
		MD5: C899269446696EB526A2401B5D12C540 **SHA256:** A996445219F0BF3A6E1A1DB98FD4487884C75C465C4D6DF50A00B4180C5103C8	
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\9df2a0168d84f72d_0 **MD5:** 7D6F4768D1E0BAFC9999748572686EB2 **SHA256:** 24D6E9FDF0A59AF238DBC9005B84688C9075FFE4503F7B237C3E3F970D64C439	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\5e26fed87f5fbb3a_0 **MD5:** F21F6E0798F2BD2158685CC2764ED239 **SHA256:** 7F13E535988B46D4583D3F2E717F659F6B36EC8265A887DC5D2D6213C4121C8E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\b7c8b4b615e318bd_0 **MD5:** ECD749F7914B4A2CE21D05FD0D432A82 **SHA256:** 12318DB23F3291CA402AB9795292E322A2A125CF5DFB0037677575C7D320102A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\81c78f193208c7b9_0 **MD5:** 2117E6E935E05875E2362C395DEA4380 **SHA256:** CDC247BBDC8EC7F60F0FA13582C835F89982BCE1339A8E058BE27AD3AF68A07B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\0434d80a3de5e78c_0 **MD5:** 8CCEDC841CEFAC52804DFA70F0F0DB12 **SHA256:** B06A90E964324085C06D2C39C8B9BC3F0B3DAA8BF72FC7D8B2911CEC90A49436	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\f7b953deb07ecc20_0 **MD5:** 9ADD83C080C27F284B17E43CEA12EF22 **SHA256:** F94B14DB37B0CDFF34AD5E419093B4DC28EA44FBF0591D0B00E5FB3FCF4C0D99	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\cb534c58bba32dd3_0 **MD5:** 4FD5420890E980CD73A0A00ADD11B673 **SHA256:** 416004B4B9CACFF795C6254725B1E1C82414A48C6564BCFF7534E7884F808A3D	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00028d **MD5:** 98B809914814E64C2D44378AD97ED330 **SHA256:** 6BDAF139AB3CBEBD6FA33D873C469E25623B700B9F10563745EB1F2EA33EBCD1	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00028c **MD5:** BE8C074E711B12DA7CD5A89F8CBB4E6B **SHA256:** A3EDF6B5E71AF32A96A575EA501AE86348B4845B9D5CD0480B47D0F6DEBA0A0A	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00028f **MD5:** 3DED8A4D9E458D416F5A6D425FF546B6 **SHA256:** 82323F784D6D40A8F3C8E5FCA7402C60226F81837C745C61EA0715DBF6BB0353	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\2de1d2dd-b02b-4dcc-a032-9547e0b92627\index **MD5:** 54CB446F628B2EA4A5BCE5769910512E **SHA256:** FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00028e **MD5:** 6D5C01ED76F2CCD1FA3ABE5C36DDC15E **SHA256:** 781246DA564B0ED474334825184C27C43609434E08D0BA16FAC7B2D3F91538DB	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000290 **MD5:** 06502F90525F16A6C12CE1D7358E93BF **SHA256:** 38A1E24263934D56A38CBD3C4650F0A3F7389A9F304591ACD7C6685BEC06E0DC	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\2de1d2dd-b02b-4dcc-a032-9547e0b92627\index-dir\the-real-index **MD5:** E4EB6FBC5E151A8CAF5DE88C963A2A80 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\index.txt~RF116166.TMP **MD5:** EDF68F1BAC2309A1FAC6051BE44BC532 **SHA256:** E5AC73C84A3C3B64818882E8A440B32DCAFEF98800FA70BBC96C7A87B7BFACFC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\2de1d2dd-b02b-4dcc-a032-9547e0b92627\index-dir\temp-index **MD5:** E4EB6FBC5E151A8CAF5DE88C963A2A80 **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000292 **MD5:** 1FA64B0B7C2078F3F543D74F132C6865 **SHA256:** 1AEC3707495549462EC4C2AD97873FF177D90808C6EA7F0FF657EC37ABFE0148	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\e1a71e2b5f89f1d5_0 **MD5:** 786810EEBA95E6EED78EF5A1E8C43EAA **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000291 **MD5:** 5BAC8A57D3616976E81339818ED2AF9A **SHA256:** 70BCE4CB4850CD99584B4704301C10592DAE1722ABC303BB1DE23205CB468673	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000293 **MD5:** F3D72ED953E060F370A1C06FCB65F63E **SHA256:** 4422EB7C523A1B6CB8234039BA26D964FF4F4245AB40A2BFD618994E7A668C31	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000294 **MD5:** F6F59A8785891C6A71506797F4ABCA9C **SHA256:** 03E8B2A41984EDC6D12616CE1DE8BEFF6826E698A43A63DE4128B19CC1453D91	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000295 **MD5:** 3E2EC228828EDE32F7CE6C5908D5CB67 **SHA256:** C04A4DA6C9BAEA05CCEDA6DFD5194B3C48105C9DCFA5A99D505A2C8770FFDA36	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\c7adfb232d7b4160_0 **MD5:** 6A3CACE7E87759C0B3374A05972A2D30 **SHA256:** 820A0E8DAFEF7CAD6EA3A464045CD4E3984745CDE3279ADD8FE5D1B6793E080F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\1c464566811625c9_0 **MD5:** 541D4587BD68CF7E15D6FD658A9DB070 **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000296 **MD5:** 224C4E92FB56864D01E2490C902CBB4D **SHA256:** 93208F4097E15FF57DDED03417751B8864E763C36CD8ACB2E3FC79897CFFB33D	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\index.txt~RF1161d4.TMP	binary

PID	Process	Filename	Type
		MD5: D98B626085B934F30F913298FBF47185 **SHA256:** —	
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\1be6528b-b619-4a96-b04b-1874aa44d255\index **MD5:** 54CB446F628B2EA4A5BCE5769910512E **SHA256:** FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\1be6528b-b619-4a96-b04b-1874aa44d255\index-dir\temp-index **MD5:** AFE30749F01C905A7992F9F465BA4190 **SHA256:** 4C073E45FB85D81AC9E79BCDC1E6B0A1E5CD732241EE74283728498BED25ADE7	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\1be6528b-b619-4a96-b04b-1874aa44d255\index-dir\the-real-index **MD5:** AFE30749F01C905A7992F9F465BA4190 **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000298 **MD5:** B63FB9513F59AE2381CD8AB67032A1F9 **SHA256:** 9E2E06368828A27AE08F7115EC40A3CE4A1828187F686E4A2165F4FD389E5970	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000297 **MD5:** 4DC6936BDD8154AE6D8D4B02FE03DA44 **SHA256:** 303550B9ECC5BDB5B80911972FE091FFCBF1E81A9D365379B0867873FBA3562F	compressed
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\297ecea5cebb5dfe_0 **MD5:** 5EA97FFF5405D6EAF61CD9A34E7D04C3 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\076d09460213620d_0 **MD5:** 6ED88F9701EB4F7321D9A03A5BF9799D **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\88e4db41ae8d6d10_0 **MD5:** 0A539C739D351513646F2ED11F71657F **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000299 **MD5:** A53D05076AA6EF2BABC5DEF614A1F2E6 **SHA256:** EFF33332C19DAE9CA76B7AB901FC259B99EB053E0FF76DAED839534F52186C99	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\076d09460213620d_1 **MD5:** CEABA27EE2DF33F2267B8BA39EE28EFA **SHA256:** A8C02C593AB57A39FA0417FFFC7D64C7B4F883DC18E10D4444F6A0E08E423416	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\7091704621e9c294_0 **MD5:** CC06283C1F9534DA3DD1A5A34242C94B **SHA256:** 706F3D8669623B6DD04C480BDA91BA34E5ED7C5E73927A25F58B7F7E2F5FB89E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\e6dd21e78ea0956c_0 **MD5:** 30D41EDA65BF5F664F1EA63E70622BF1 **SHA256:** 32EDF3CF129EF7F36F46B2169F2EE011E952DA55071449F5A269DA4AACCAF63E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\7091704621e9c294_1 **MD5:** AC9099C83DA14A0482AACE084D2B3AB5 **SHA256:** 51A8520CA2E8E4B2F16C65033C61944E624D576FAA28062C5FE08C1F10D4A294	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00029a **MD5:** 856A44C7E5F305D914F73151E46348F1 **SHA256:** F576EB2ECC60FE36E8222E836AF2B7A7FC0E2F757159E970631EB2E496B0411D	compressed
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\297ecea5cebb5dfe_1 **MD5:** B1FD40AD30C2EF72F80A2096817593C6 **SHA256:** 19AED031AB7FEDE73B6A6C0FB72842E42704D299282D1C63A67C0ED11586E667	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\18639971391ce52a_0 **MD5:** 4F730E31BDCE967B6259685D1F662557 **SHA256:** 8B465941E8687871386C83E5AB28EC7017CC8B965824D0FD537DAD2AD591B2F4	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\e6dd21e78ea0956c_1 **MD5:** 1E433555231CA36D6E6309C47CB1E9AE **SHA256:** 8D1191C81A49ED057991FD9FC0B92E5A68604370AC3BA498931B5A9CF39CAC1C	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00029b **MD5:** AFF4210BCCA43C834A38372DF7AE19F7 **SHA256:** CF6FCC2609811B3FD38D025E741B26ABA6EFB0E8245201DD81D5BF7597027919	compressed
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00029c **MD5:** 4866AD1773F31068BEE93859EDB477B7 **SHA256:** A59A3030EE28FF95D79D8B8E5281A7FD0C2DEEA65F0CCA143AA7050A7AC170C4	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00029d **MD5:** 3B25FBD9BE0594E7D5DD630003EF4194 **SHA256:** 0AB699EF1483CD423E0880E48701EB0F38D8D250A4F7E63262A5A10E587F6DF1	compressed
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00029e **MD5:** A673A4FF37878AB1CB36ED1079A6E033 **SHA256:** 9EDBC2B7D4862BEB81DFCE14AE3AE0CC1DF4359C2B535A79C34F4CC5072AFA17	compressed
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\38a1e16bf8766042_0 **MD5:** 10F551D9BFE00923CE51839859C93A04 **SHA256:** 22B00F10CE1C8683BE609A307BD3C45BB7A25E212BC23135859D8015B50B0216	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00029f **MD5:** C99F966767A99C2971AAAD4890F0D323 **SHA256:** AD5F0DE938A628DF6B0DE66005E92497BB39C09FB8491EA7FC4D5AFD600262E2	compressed
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\0a10c972085c7402_0 **MD5:** 763D094B71F896BBC2B950E5E596247A **SHA256:** 4F9241EEB4AB76DB1FB4597CE2F80296A7DF84FE6DC78BEE8C3C27CCF4D16961	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\93fe915ac9be3fe7_0	binary

PID	Process	Filename	Type
		MD5: 483595AC4CD6CB1381234F22996BB6DF **SHA256:** 0D491CB18EE6357571AB78A8BFC049C9CC05C32576B131D250FB1CC0DC299A4B	
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\38a1e16bf8766042_1 **MD5:** 7D4B967BE3BDBDDB31CE25A8FFDFE6AC **SHA256:** AE3ADE70FD865745076DC601F3B54DA301044288EB7BAFD323BAD03335798480	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\7e637e1c21dd0b8e_0 **MD5:** 0616DDC0062A7C017CC126AE54C23943 **SHA256:** CEF7195B9618901A1FEBE66CB4F8F76E090AC7E5ACC9DB00B6550F92ACCEB404	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\15762f8815377cff_1 **MD5:** CB96A163EA4EE3DAC56CDCC73B43D0E4 **SHA256:** ED97174B628E6BF19E94F2004C95030C3FD1D9C2734FC5B84CD2CE6C66019C83	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\3cb867fd889a14ad_1 **MD5:** DAE9B1537FD42283C6C3E5F8D3525969 **SHA256:** 5599D484DAAD4AD2010ADB048EDDEA4459F8E2C177C149D7D4F3940A088DADED	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\15762f8815377cff_0 **MD5:** BC99E18B51ED2A878D63F12A1E0DAD55 **SHA256:** C061F440F5290B647CD942DD25FAAD85593B0435F783FEA84F54EB141D119FEF	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\7e637e1c21dd0b8e_1 **MD5:** CB6FB5B9C97FD7A657EDFB29B423D74F **SHA256:** 84CFEF3F590A60D7D9463A1BC81FD80C2A04924A3225816107DE5AB6DEE49246	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\5607282c9773cc94_1 **MD5:** 654E9BFF7B1EBA3AE9D17EC69A58EC12 **SHA256:** 7F17663EB73273BF158B947CE6DD42C8F9B5CD1D76652D53E12924B9AF577800	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\3cb867fd889a14ad_0 **MD5:** EB827454381AFE32E441D4AE1793FEBB **SHA256:** 708C36F2A1089079C494E9D936AE3BABBAF9727590A7B4C6B3BAF6DA3D9BE6AC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\5607282c9773cc94_0 **MD5:** CBCDB49CB9AED6F88B5BC5D53387F0E9 **SHA256:** E630AE342AE486460104C435E935133A7646BA4CB72D4B5855CD5444DD8B43BF	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\0a10c972085c7402_1 **MD5:** FE32DDB387DDBF10EB03C9BEF41C8BF9 **SHA256:** 6AFC2BA7FD34422377FE67531FB4724FFCFA564B08AD027C1C7D37B9966E2451	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\f6cb312cbf1f7183_0 **MD5:** 509304671309A5621884B753E5328714 **SHA256:** BDE398F35F210D27A579A0A6EF02A654779F8988196D065570411E1AF85707DF	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a0 **MD5:** 5E390E0BBBBD5618E3B8E85C670CD2B7 **SHA256:** 4F88EB22CF12C7E4F44D2A02EC43E5F31B27E48D0258C159548D244A94C8330A	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a1 **MD5:** 6A1409F3BFD182F0BC0FDDE83200A6C2 **SHA256:** 6231EC53F75B0505A327B57EA314A3A7454101CFE206F05D16E4A62504312186	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\f6cb312cbf1f7183_1 **MD5:** 6714C2D334E76F0FDCD3022CBAF401DC **SHA256:** D3C4F441FD2071F78251FC171FB1F6E4E54D228137BCCF7B8A6B8CE569DFDC71	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a3 **MD5:** 8B37E17E2AFEA90135155708D8B2C5E8 **SHA256:** EA5BB2B4F55A2DAA3F015FFDDA73D83232B2622BAA7D23A24BEE88878267DA06	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\44db2a98b7cccafe_0 **MD5:** 07A47A82A5FA123283A7F2F40368BD8D **SHA256:** 0ACB8208E5804FEC517AB4C55C2A327EDAF444D43794E87B2DD5827CE1127837	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a2 **MD5:** 8A9769FA68D3B8C31880FDDFFD90C03A **SHA256:** 0C3F348B023672A22E925808A434377B846656A53C0133A3FA92D8263F1ABC42	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\84dbfcbf900b5662_0 **MD5:** 6987B1B4833A24F09F558A1BB40C1ABB **SHA256:** 7C76F7CA88467A3315571D1BD4ED8E9CBB1C7F9D802591EB89FF8AAEFFC3F275	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\04c223347457a89e_0 **MD5:** 134D759A0130CA344659582FFD52A67A **SHA256:** BBD6B0FF2B7ABA2FCCA0AE0F0619F2244A44E6E46A675D44EB28D971A4393E91	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\04c223347457a89e_1 **MD5:** 443E844EA1CD181565A2F69620652EB6 **SHA256:** 76D85FA12F611A0B36E8AEC56E26201C38BFFB0D1C9F7024E62C526C457FED3C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\2949c11b1a77090d_0 **MD5:** 9A65A0A8462A2CBB6E6E24658019295D **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\2949c11b1a77090d_1 **MD5:** 20783D8B1ADF96692F1624E656F0ABB9 **SHA256:** 0E78D74D3B049A541DD013BBF9B1E57B07ACE964DA4F35643DCC56E61AAB9DBD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\6a9b325a73f73749_0 **MD5:** EAB4B6B31545592998399C51402B72B7 **SHA256:** F3B97BD329EDA338DFA9FECB247F0D55448A49993E894353041B3860F53D21BB	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\b8f66e5fe9246dce_0 **MD5:** ADB688EA13C6C90A02E3179C2EC65D45 **SHA256:** —	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\eec3b734cb3516ad_0 **MD5:** FDA3AC557F48D62E6DBD1EAF4AA962D2 **SHA256:** B0D057F7746EDBE06A9D4A4F40D74BF2658E01076A2E2C1C19EB34942219751D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\6df1a24b987e9b1c_1 **MD5:** 84844F0777BAB82568840B0782A2B1CB **SHA256:** 6813421B5E0F46A9D9EC13C3CC4776994602843967F1A556045EFF3CB5491220	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\ee2c8dfe66c43c03_0 **MD5:** 67641E6A3E4A5C77408AF824BA8E85AC **SHA256:** 29B1DEB1D6BA8043AB70036264014C762455CF773232E8A000800B393446E837	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\6df1a24b987e9b1c_0 **MD5:** 612F2740A94D0C8E3B04EDF067B43ACD **SHA256:** 8490BE9476C525B60E720B2D42A1072E6188EC0DC1A51D813217CC90063C8B1C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\eec3b734cb3516ad_1 **MD5:** 5680AB506876948880ADB5ABB8DE41B5 **SHA256:** 17A837D8FF5816A307582A3C1B475D21FF1AC929C2CBBB58387F82FB4D5A7184	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\02038bb13b1de99a_0 **MD5:** 8DE07818F9B6B640C6AA15E5B07C80E0 **SHA256:** 0AC808E302C8353D517247B6A6A716E45A1D2DA75FAD0B6A9E37FCF97169DBF8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\02038bb13b1de99a_1 **MD5:** 83CDED7F26CCB1A23EC9B6DE8202051B **SHA256:** EED9AA87ADE5C5D400ADEB110C23BA95014ED3F33C0C947EEEBBB50827FEB9D5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\ee2c8dfe66c43c03_1 **MD5:** 429753B5141FF20C258997C7E676551A **SHA256:** 7992F224324341DD5DD0C2FE0D27CE73D6F0D60D93CF125C635D56A6DBC4D62C	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a4 **MD5:** B89E9D7431247A8209E78884BF68E6CE **SHA256:** 1AD92B457547DA047998D66793A4F6216ACAA9584A2EC31A49A5D1AEAD7CA4CB	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a7 **MD5:** DACE0310F47BAD8382DBE21BF5361F13 **SHA256:** C13DE94891CBCC8406C31B3CF33D88C80A4EADCFD767A00EB7B5CB34E4237362	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a6 **MD5:** B245C7042CE327CCD52AEC89FEF55BC0 **SHA256:** C4CE59AF1B80BA2E03212426DF7D3EDB94E5C24394DCF91DBF0FCB8BB2B0923A	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a9 **MD5:** B5337E69E6AED2112992A14C078CB549 **SHA256:** EC6AB21E0137C6FC1E3604F45985796B0E932D59A69428C14208DDA62DB5CED5	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a5 **MD5:** 99AEA5CB6923967F2AA9C5F2532CD10C **SHA256:** C094B370493A8F948C7DEE654B9AAF88A6F4CA3DB6F0A7AAB675A5D7E28B2EAB	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002a8 **MD5:** 4B3CAB4353C2AD912D3C8B4A1C9D0FAB **SHA256:** A642F8BED01E2BD65D12B62ACFA609CC02D18912BF40A3D13DE1DF39BF69E79E	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002aa **MD5:** 651E4C2FD14E32E0092AF2B9730A5CAD **SHA256:** CD765E175597E930C09348BA4A91FAEF05BA857079A4B7A74AD336423820CA4F	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002ab **MD5:** ECFB49AAB1AA7C864B122DA5AC42A3C1 **SHA256:** 2E922F97D4DBFF93A1C8B89724B0F15195130D76DBD69DF4B2CB6D54CA2E621D	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\84f78fade1d89a3a_0 **MD5:** 914E39EA05EAE1CB1DD0D23531B7158F **SHA256:** C72B545FF3B1F8C65A527DB9F2D83316C205C71CDCC3CC0E1C82667DB321F811	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\84f78fade1d89a3a_1 **MD5:** D25BA0F120111210F1D11F0E4D27A2B4 **SHA256:** 756620959B8EEFE036DD7EA3BD31E4F241BB392848579A746093B120FD7150B1	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\ced7fe835a8e3158_0 **MD5:** 34FB99A6BFB2CE459C5E29F21D2EF38E **SHA256:** 1AAB8AD9DC05C98AFC4F38AE94AE2F4D2B0F6D113F7881CF54455247C5882886	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\dfb05e0336105981_0 **MD5:** 45CCF1FDC36781EE0D536C1AD317EFD3 **SHA256:** 08A6323A711FF64D51B625D29FC861D3729DE8795A438070A5CC863F59773E1C	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002ac **MD5:** BD2A2404566748F804D3B49487906439 **SHA256:** 483F20ED415D6FD09889E60CC900F9EB88A0B7A7C9D6DC05A4B9BEF4DB3FC107	image
8852	msiexec.exe	C:\System Volume Information\SPP\snapshot-2 **MD5:** 84C83BE729347DBF72A54CD25794BB53 **SHA256:** C678E208F0B02D19B9462D638B98C94A5221D2F07E96C60EEC97087D3D8F19A6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\c95567a970f2d095_0 **MD5:** D027E4291064F77C3305028BCB597AA1 **SHA256:** 3A962D2ADEB061342403295E7B62515C2F1B6E34BD23DEDC4C45A2312AEDD919	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\3a64472f77a86345_0 **MD5:** 3A35243FD56C19C79A708C33C4F9DE08 **SHA256:** B3A976A398B8EF87554BAC9831F7E9BB563A6D11A233602AD99DC7245EB175A4	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\21eeea2074dc62ea_0 **MD5:** 5E074BEAC0698B830E11B981B1750144 **SHA256:** F2F8F27A850F061397B2BDF36430FFEF9EC3832B46833E1CF022466A3D7B5D08	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002ad	image

PID	Process	Filename	Type
		MD5: D1F5F908F482567ADA844D540CC56419 **SHA256:** F1E92E71686320511E343201F3624F6E5608CB106CAC2EC1B131FEB4C8F7B33C	
8852	msiexec.exe	C:\System Volume Information\SPP\OnlineMetadataCache\{3e43f960-0ab1-4416-bf3a-b0fb614d9350}_OnDiskSnapshotProp **MD5:** 84C83BE729347DBF72A54CD25794BB53 **SHA256:** C678E208F0B02D19B9462D638B98C94A5221D2F07E96C60EEC97087D3D8F19A6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\c0fbe0ecba765527_0 **MD5:** F3FB67FA2EB4F8FCF08216EE50CA9D22 **SHA256:** 69A0526B17E879F456D5DAAB07C631F23AD762FDAFA5BC1BBAF5DA40227D1721	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\4f10af0764437d14_0 **MD5:** F29F423EC69F3D2B13EFC310EEB2ED60 **SHA256:** 47594092405151FCB5EA20623BB3BD7A0C24D93CE388341BDB7448C0E80AA3A5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\cc111027181b2619_0 **MD5:** 81F8799A811FDB522C2608DA3CCB8D49 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\a86e918acd0f3b7d_0 **MD5:** 637E68C841AC8EB6B719ECC6ADCFD412 **SHA256:** 1041D484E163759B84894B3E071A6DCB67A2E3564FA15AF7B0DA20097F5EC490	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\cc111027181b2619_1 **MD5:** FC08E0B88D46E71EA90F0B8AF3E1C283 **SHA256:** 72E4C6C52F2505EB8922DA4AB885FBE0191CC78B6D72E3A6F9A6A5E2FED70066	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\94dc64adf82edc8f_0 **MD5:** ABBC64027503E97DFA34F34530FE018D **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\fc444b244ba9b7a4_0 **MD5:** B2EFEF6F7DE9D21A4BDE2433B8E3CCA9 **SHA256:** BCC9266F985507A43EF95FE9FCF905C485A4C9376CAC8730FA2771D447464466	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\637929cd1328ab58_0 **MD5:** 7967EF586AE1B71BF92739E3F31D4548 **SHA256:** E3188ACD2C5CD2FFD43F6DE2B1409A1B21EEC11F102FC4089E82B4218F739565	binary
8852	msiexec.exe	C:\System Volume Information\SPP\metadata-2 **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\51c5709c1d898cf8_0 **MD5:** 05FC502469D3E6F0B598AACFF1F41AA4 **SHA256:** 8D34DEAA10F65D090ACDF4B018641E747FE59E8C745E2AED345C2E8D96BAA107	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\13c1736ccb839860_0 **MD5:** 13AE6D3816D767D6ACC0DA9ACF3FC2B2 **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002af **MD5:** 48BDAEBEA0B4425A8C41B453513CAA98 **SHA256:** DDC0761418EE739E0045E903EA5C5DAE0503C6F739635A7230B8C6FE205943DE	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b1 **MD5:** 3F589E2CF60DBA0415CA3553B6F9B66C **SHA256:** 24247029DD97ACEC99D1DD8C7278EEECBAAE00EA792C542BF680D2635B8FE8ED	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\866953eee33d0031_0 **MD5:** DF115CED2E6A9A789D92573013F134A5 **SHA256:** 9564A949B858CE11E66233D7C73667A2EF3F881634BA0EF3CEED61F1FD14BEAD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\31aca5ff58d0dbec_0 **MD5:** C4A2F12F8DA5B223A2D3D001871FE094 **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002ae **MD5:** 81CC08855B9AB73A933C9EEA8A7BB407 **SHA256:** D981F015ED4502909F5B4EF02244DEA604FE12E23A4CCDBBE3F9AE2DB1B057B7	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_ntp.msn.com_0.indexeddb.leveldb\LOG.old~RF116936.TMP **MD5:** A7468A8E083836AA1B72A5A23CEAFF52 **SHA256:** 6B1BC16F07BDCAC7F4E94CAF88FF1606ED7C71C22DAC01564883EB30A8D2595D	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\c81d941f6bf79e96_0 **MD5:** DB97516BD6FC4259D0B948702185EC80 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\19e1dbebbda6317a_0 **MD5:** 1E638D3A192F9A21AD92C85C2AA0B6CF **SHA256:** 4C062023E54478A1255BB8D1412035933A2001E29F168594CECEFB34822A41A8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\1768525a9d0b39d3_0 **MD5:** 274A6AD8A61CF6FBEF525B03EE3E418F **SHA256:** 2A65D9E090C5E20F39C3AE9972B005D12BC47ADD21B41C5E4D056CB5BE96ED54	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\63cad7be457a945d_0 **MD5:** 3FA524B24357D18C1347A854E45BCFB4 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\de890e1fe0902c96_0 **MD5:** D6AAC9EE05C0721B4C7D68A7F4EE50D8 **SHA256:** CF520E1F6B1D2A7126638E1D5F78B63E1FAAF9B290C4D9F334A83D0905917292	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_ntp.msn.com_0.indexeddb.leveldb\LOG.old **MD5:** 0825EBBC01C197BB5B336E831FD36F4B **SHA256:** A49FE56A5A4AC6EB696E78EFC5BB59E7C78EFF54EFF8CE48482020F72B4D10FF	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\1be6528b-b619-4a96-b04b-1874aa44d255\ee91b116cc2005be_0 **MD5:** F5D9D81D26E5EF2F6771A85097BC01E9 **SHA256:** 1DD2BAC1E8C694903DAD39C0CDD6060D953333851599E7B83ECD8AA593A8109C	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b0 **MD5:** 9D39BD32C69AAEBAD4D0EB934D73AA80 **SHA256:** C3C21CEAD863B0A32F50010683343533D3A4E007379E0468E2C35B00DFCF911D	image

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\1be6528b-b619-4a96-b04b-1874aa44d255\todelete_ee91b116cc2005be_0_1 **MD5:** F5D9D81D26E5EF2F6771A85097BC01E9 **SHA256:** 1DD2BAC1E8C694903DAD39C0CDD6060D953333851599E7B83ECD8AA593A8109C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\22755a87bf952882_0 **MD5:** 61320E1866CEE9BFA459A014B97DD3AF **SHA256:** 63EDD3AC1C82FFD0B211E3AEEB38E1EAAD2037203A64112CBD6AA0071EF46167	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\285ac031fdf9dea1_0 **MD5:** 251A501661588CF11CB9BDA204B5E4D8 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\22755a87bf952882_1 **MD5:** 7ECC417A6264774461FA9A8BAC5A7252 **SHA256:** 7918A8BAB18F2E46F50D261E62DADAFB80B8EABC51B1149624EF11A936473DC9	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_ntp.msn.com_0.indexeddb.leveldb\000003.log **MD5:** E1AFE2022986FE5386AE8A63E3DE1251 **SHA256:** 2F80FC170273D3E8CB55E50EE0FC6B60883BBA29964F8F3B0D01D6D2B69E3B10	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_ntp.msn.com_0.indexeddb.leveldb\LOG **MD5:** BEF39F127847C1F2377F91C0556E99E8 **SHA256:** 05AAB9BFE3BC43AD836B96CF9EF9525E04A505C9B9C9970861C8F0421788BD74	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\285ac031fdf9dea1_1 **MD5:** 3FC8E58BBF8394827E4F77136EA8BDD3 **SHA256:** 65BD841F75CCB9C04DE65AA1022F47AFF42D36CC71633E7D2BE71E934F404A73	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b2 **MD5:** 2F475E582337BB53AC92748555FEF51C **SHA256:** 28DBD5C118765039CED355B87122F42E771404ADD0CE5BE9397C3B38D8CF3B7E	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\bb8251de83eed03d_0 **MD5:** AB6A11A5BE2CA09A93B6DA7646084C25 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\e8da6d142c9a051d_0 **MD5:** F216CDB5C12365E508E45E5A4ACD6F23 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\343c3c0e7c2273f3_0 **MD5:** 3438B95E8FF9DC43D7EA9EE14734C706 **SHA256:** 4F7FE7EF2D7FBCF59CB27A614EF8879CB40CDBC9C72D606C293E87BD8EBCD284	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\b483ff36f3ab4d89_0 **MD5:** 4CC58A28AD48403ED5ABC1B1378B4681 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\4be624c95b6209ff_0 **MD5:** 172A93282A780C096212DD91AB5F646C **SHA256:** 4F35BCAFAC098BD02D2C6F8DDEB2937C7F13AA189E4EABFF88E59326D1D7E7E1	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\e7446e3d6aad3db0_0 **MD5:** 7A16C621AD18E75C3E53D44814DED4D3 **SHA256:** 4B9F52932168F68CB6AA51A10DBF471E97139DF67673679A03A8511C84652FF6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\411cfe64203da124_0 **MD5:** DD7C3DDB36599E4040369A4C3289B0A2 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\5141051f1cd5c762_0 **MD5:** 0E7A3DE2ABF5A7F59ACDF0CE41574958 **SHA256:** DABCD47DB80E6C365B3C73CB80A2F15029B18BC5DC0889D2D39195BA931E7FD3	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b3 **MD5:** 2EA86888CFFDC9FA78756DC2EE6877FB **SHA256:** D7CAB57401D560FDED725FC6C3DAF444CB1897C578F422936153A5FA6D1C0D61	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b4 **MD5:** 8F850AAAFC8DA0DF7F8F0A0B682A934B **SHA256:** D40CA516A00F4B6AE9937CF0EAA8E1F0C2033AAF783DAE3C461D68B8B142BC4E	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\4be624c95b6209ff_1 **MD5:** 3BE903AE81872DB5216273105118AA2E **SHA256:** 1E29DFE6B2728392B6DBE780C63A579533830BD6B3B5FF92832A45475DA52ED8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\1f6a15d3811a5bf6_0 **MD5:** CEEE85A0ABFD88112B91D2C758693237 **SHA256:** 9CB84F3DD3CD2A3DC80B17F06802BE9AEE06F8D0686AEA3637AF41AEDB45BEEE	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b5 **MD5:** 65A279C1EC9E31FBE526F5739E6E3C4E **SHA256:** 1C66F10233682CEC48A00C59CEAA74CE09E6970C6E9F69BFFEC7448D75CA3236	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b6 **MD5:** FE2B530B26DF63025E963A0057C63BCA **SHA256:** CF25DD0CECFFD06958B35D624B38338D52165F1D4EFFFA43B673AF7C4917FFE9	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\95320d110f386319_0 **MD5:** 4CBFA9D043478E38E868F11DFFB74D7C **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b9 **MD5:** 87F12BB17FF7656F148BDB072AE6534B **SHA256:** B59F1DE014D92A7D354E5CBC08F37DC9DD53F35A65958CAC5D499F108F857150	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b8 **MD5:** 333AD73AE520A1035C68E569AE85D54C **SHA256:** E113B190867F7E4A2AF7AC8F8924A58B26DE6DAA303EB2A672225E7C2A89B89A	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\9d1b04d6ce180287_0	binary

PID	Process	Filename	Type
		MD5: CEB30F61C06F23DBFF9D997534D92A85 **SHA256:** —	
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002b7 **MD5:** AA843ACE6A4FE9C48AA11707EC8A2FBC **SHA256:** A3FADEE4809A33C96DC7CD91E7C521A4C9582DBC996D4284B0AAA36D0900FDF0	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002ba **MD5:** 91E6C61B57A398314DFEE0C5A672DE3A **SHA256:** 8CAFDA33463A4308812D25B2428970D7963562DD83FC54EE5BA37DFEE500375E	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\9d1b04d6ce180287_1 **MD5:** 133EB6410A9E4C8DAD406C7F2C148FA1 **SHA256:** E73BB90FFD7151184899963584E8313E7241176218F8A78F25ADDAA132F3B175	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002bb **MD5:** 8F250A8A9272B16334EC75F930487A25 **SHA256:** A4D67FC1333423B3D17B1B170117C5B4452DCD5553F7160013D2C27C793F8BDF	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002bd **MD5:** B73808712031DA88FE918FD01DEC378E **SHA256:** 2B2511C9991588ADC9A1F6F415AD69182868559874DBE8C0C565479A95CC0E89	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002be **MD5:** 952C8383954603514C6CB86503D6E5F7 **SHA256:** 7261F1701C2879128581234D80E3FAB492077C9A063B7443CBD734D722D4F8E7	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\992591c97294e836_0 **MD5:** DEE60A29BE9D90E62D5AA238EEE479FF **SHA256:** 6328C8F0B069EF01DFA1532F4A52334879B25C6719B105B274FC8E1224D89AEA	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c0 **MD5:** 418186F15F29B85479F8FB6769DB96A7 **SHA256:** 3D18AADCD907EBE7E2F8F0A5C7B232894A8B821934107C441E691CFC6B9A926D	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c1 **MD5:** 8A87419A1206B512CC1FDEA1076B1895 **SHA256:** B8E854B9F8F3902CC6A5484C905421F50F28BA1C731247E9DAFCD11DD6385C08	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002bf **MD5:** 8367AE57108C4340848EB1C39A56C030 **SHA256:** C5545B3F5A02193FC9859E1F61286A2F7C11F6DC31BC4FBBA62EEBA612BE6A52	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c2 **MD5:** 4B765D1EF70B9CC56777DDFA677DD16F **SHA256:** 55BC3AA5571CA5596A0DDAB8C2C0EAA06BC2F75C84129F3AB38FFE0C60B91F06	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\09cfd9f0284d0e82_0 **MD5:** 48720A6CC6E7D8882DFC307D9D3654EB **SHA256:** 98BA2C6076A5E160433A4FE7FAB38788F1D6D093E01D48D525DDF3D8B20F92BE	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c4 **MD5:** CF00F411B8FC833E044F12840F255F9B **SHA256:** 65996A8C62A411A04EFDEB5BED8994943F5B7796F0EF41F8481EE09F5D08C0CD	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\09cfd9f0284d0e82_1 **MD5:** 9393906BE7B21020B4B963E1E5CDB610 **SHA256:** B30D48BB4B90F90D2694F6C1269C120592FD385D32A1FB9893A40F9A5B127E64	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c5 **MD5:** 91987D353EDC18247C555E00E5570F82 **SHA256:** 783A7EB0AD992542C84AE0062ECCA743FB32B63794DA18172B73580962C21223	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002bc **MD5:** 88FBA4B10D986D0DA12604B530DBEB25 **SHA256:** DB8116F7813EC467F5C7536472AEB41A9769EE92F4CEDB5EC03098A24B7EF245	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\baa3c9c32f51e5c5_1 **MD5:** B7B266AFD59BA550E79543A07409687A **SHA256:** 9ADCC02B10A8926D55E77702FAC2EEA828F8CE60BDAB340DA1007EFF0F5DDEF4	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\baa3c9c32f51e5c5_0 **MD5:** 90568CAA5E35A2CBE29865C679C1857C **SHA256:** 74E43BBCDA41481FCCBDE65233D0F744D2CA85DAA10E2A5B23CB83C574091A54	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c7 **MD5:** 79593B4C6D6AE09052E0046F79941274 **SHA256:** 6F5D5CD49483C7D28A2AD88396741ABFF78C25F094337FF5C30E69530267ACB7	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c3 **MD5:** 21905C192DA74E4659B420CFF198AB24 **SHA256:** 9A1D5EC662544EA6E0DAF22A8D0827FE5DF4F6B1B13DC8D839B9958D7D77C2B0	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\17e4013a4d06c770_0 **MD5:** DC58BE607EEAD79E472F4043B48E026C **SHA256:** C3ED2141594099EE86715513CC40CFB9FBE993838230E1235A8F9079C9DA3BEE	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\fcfd85c77df0c950_0 **MD5:** AD8A6C0999C5AB83961459CE79A41C5C **SHA256:** 0DF041E89DAFD6516B565F5F6A33DA4BF879A0C69210710386ADCA184EA20F3D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\17e4013a4d06c770_1 **MD5:** DB04A88EB2E4C2587D8A0567A88CE2FE **SHA256:** 36A91241B0892C79BF715310534D2CEDF6DF806E5C7B715BE1975C7555257AE7	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c6 **MD5:** 9A0FBF7DDC206DA3A5EE1AAE1EEB06C6 **SHA256:** 9CF4F7D550B83ED4BF340BF07296D12195FC3B8A562A7F0743A3A1E0E08D0CF7	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\fcfd85c77df0c950_1 **MD5:** 60182814F66FC05BBA34E70B8F190365 **SHA256:** 5504A20F6C82E321CB8A0A3174687CF31761AEB076C7B36F002FDACA3EA7C054	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\42fb933176677e91_0 **MD5:** A3E4DCFFA51D4C001E148896A33F8269 **SHA256:** 2FC53770E3D5825B1672F7A77C797F9973921DBE7DB4FB17CC2AD9C57CCB8C67	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\725bbb99ef17a5c1_0 **MD5:** 6E7F50A87478F5EAE7F82B1610DFDD91 **SHA256:** B201FF64B66F405B88F2DF9B473636E1281BC6B734CD5C6071740141444D56DD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\52499ed7c79bcd23_1 **MD5:** 512D57B0335CC355830FB11DED483C6C **SHA256:** 2756239A5FC60FFAAC46667496B273AEEABC7A88D937B44DB7F6EDAB5A6C96EF	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\42fb933176677e91_1 **MD5:** 2E54971AF95182E43B7464A96F5D2B70 **SHA256:** D221DD408E24256D72C135A5FD8700CB8B6DAFA9EDD1F05DAB22D50A222B8F39	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\52499ed7c79bcd23_0 **MD5:** B2DD5CF9FA82E2D25A7A9A691F22DD3C **SHA256:** D12416FAA8E22790DBD2E3CFCDB5C9A8044D942DAD71469BEE9C05AFC39E70F1	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\c2e8beeb5ecc4566_0 **MD5:** E57BD916205F19496B3B5F47E874672F **SHA256:** 9FFAA7D86F8D16AC5B41CE027769A1515C22EEC1DF1DBACCD95D14B6D44B9962	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\b3c2fba4d7c94f02_0 **MD5:** ECDBDDB9EE7184644C13BDB9DB076083 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\b3c2fba4d7c94f02_1 **MD5:** 6F50058AF18E17FE8946A7F6F10E6D49 **SHA256:** 400E45751588026A2B8AFDC2ED91F92EBD35BE2D7DFAF2722D23ABA4F7BC1300	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\c2e8beeb5ecc4566_1 **MD5:** A2B703ACC0BC4DE326E97EEECCF3ADB6 **SHA256:** D38A3DC6514FFF9B5270ABCDC0D37C83722F8B5DAED7D5E7BC700E4ED66F6A1D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\1759f8fa159fb1d4_0 **MD5:** 3CC4F1B29DFCCBEF32035F08C889DDCC **SHA256:** 3E9EF8A6CCCC3CCA67AAF2F52C10F0E1144B5302D4ED4D7391825724965C097A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\ddf4ad1451f6d37a_0 **MD5:** 16B6214D3468D44544A85C091BCB201A **SHA256:** ED7EC6946E7EBC7E4CAFDBAADF5ADAC71EE4B5671B1924C6C77CF6D3BEAA8C19	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\ddf4ad1451f6d37a_1 **MD5:** E242BE25B71CE7FAC9BF2E81E1CA042B **SHA256:** 0C4469BA898D4FD2AADCABE9F3D2345EE7D97AA1513219EB5EB26F7CD34A9097	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\1759f8fa159fb1d4_1 **MD5:** E178DD92179AD4CB4B5AC55202337874 **SHA256:** AD9CA07E99AE36A215C6F6FA54CFCD33B99A689333C998946B464FE9A6AD3EAA	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\f13610671e28ff7f_0 **MD5:** B15A6D7C1E49502F909D3B348598C3FC **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\1e20c7d19e0afe1a_0 **MD5:** C40E6D9A158119509B81E23B02865450 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\f13610671e28ff7f_1 **MD5:** B71D58EE5DADC329E90E24CFFD53ED35 **SHA256:** F1E11872E4D68BCB948785B7FB073DFC6C104EEEEB25084B1FCDEC064F0B0A74	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\10b0fc57faf87af6_0 **MD5:** 9CE6186FE5EADB25A757EEEDE46AD4F6 **SHA256:** 945955F64272D0BB5C07AFDAF3ED84794C6642B43E07222FCF530D292703C057	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\1e20c7d19e0afe1a_1 **MD5:** CD8BB369B40110FF29464E4529E4AAE2 **SHA256:** 0647C0717CE83670F0EB1921679106DF24B94D46EB3233A6603ED668348B09F1	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\10b0fc57faf87af6_1 **MD5:** 46A4E2ACF6AD60121410D38952C3AB4F **SHA256:** D98ED50107656A3D0247C38CC38E14F0E6342C223C51B551151486C8F90EC3C5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\3aa5ffb927447822_1 **MD5:** C6C5E2A88D0FD0013D8133B5D64A6810 **SHA256:** 569F76CB1905F7A4848F9924F720D1834916272E6418421B2082C0A98D67D398	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\c43789bad7918fdb_0 **MD5:** 7BE58B47A6609C1F1D101A824B08FA71 **SHA256:** 7DAC0D644D4BA234A024B010BA814F6F77850C208E4D10F74A5C9A8BEBB1662E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\c43789bad7918fdb_1 **MD5:** 2BA3F8A3F3E90E12BED726383DAE912B **SHA256:** CE638D4707C8060FE8E0EF00B9C773C4AE1ED17270CDCE6987386451F0BE3B5C	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c8 **MD5:** 545357ABFDF45AE1E66A3FBABC971D5C **SHA256:** 31C3D32749AF72B2CEA34E55B996641C7BC8092E4C2DB1D91C479BD44BB667B3	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\3aa5ffb927447822_0	binary

PID	Process	Filename	Type
		MD5: 342BDD0610128F850839746AE602B964 **SHA256:** B1F9BCF38B7F58CF13CFC8DDA42A699D8F8435D5DB2D4CB3D8429668A593F6A9	
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\b5727af68a64ec71_0 **MD5:** F9996808FCD1118CEAE9A31AE1FFA1BA **SHA256:** E47D084463CEF2BA091DC3BAC45A910758084B957C8A1C4262372970843BF692	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\b5727af68a64ec71_1 **MD5:** AA494C98E8826BCC46D5BFCE6CE562FD **SHA256:** 3CE3047BDF81A2C7BBB7660A27E6DC8D7B0A0EE1342BC8D8C655B92F98A19B6B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\ccd85685f735e227_0 **MD5:** A68E355A688AF3C2FE89B056F02D1015 **SHA256:** EB30DF008C1229E4D94EAA28C2E137C31F9761A9996FF8186F98CA50AD3D8719	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\7b508ac7ed278d62_1 **MD5:** 9D5B0B5CCE518F9341601FE28F3840F7 **SHA256:** 9E2CF8FD1206FCF0CF87BA78B5A0AD35B179EC747DB2DD4A59820215ECC1F38A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\ccd85685f735e227_1 **MD5:** 95323E064AA0DB36C8BC7A04FFB1D9D9 **SHA256:** 4F1DA759B7A62F0B0D087FDC14055FD14DE1665D5B74654190E2323EB73226B4	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\7b508ac7ed278d62_0 **MD5:** 7F897E5E84B436A8B9D1B3F6546AD1ED **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\070fe3567a312bbe_0 **MD5:** 9F45E0BB86EEC218D32BFEA9C8FED2AE **SHA256:** 8F5A52BA3455A16D76BD7F4C7660559EF214B7794B546BBD6665AFB408A8223A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\070fe3567a312bbe_1 **MD5:** 5A9397F8045672936AC29C6E94208598 **SHA256:** 5851BDD014940336253AB51871DB1655FA2E5B7391246BA80EA124A5B3848F6E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\19a1b0829885d278_0 **MD5:** 43BF1248DD4D4670944A68F6458E6191 **SHA256:** 7DE6C1BDF65530C109BE2FBD44637FD0F88A757893BE892467EE6951EC2E08AA	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\65af2891b31bc96d_1 **MD5:** AAC2A5B5A70786AE0E5E3FBE35FC2059 **SHA256:** F8ED19ACC17AD49A50879CEB03E7DF8CEC82C5A9265FCC380CB9EEDC81ADF450	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\65af2891b31bc96d_0 **MD5:** 86D1E9822653A1F84DD29E096CE9171D **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\5200e5fbdb444ea0_1 **MD5:** 15A80C8E626CE2BDDE6665BC1F03E972 **SHA256:** DCA17D0F57FEC2F4EF83FA3EED8BF6B06A98CBE2BE0A363840B6F837132CA0A6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\5200e5fbdb444ea0_0 **MD5:** 27D5BE3D63C958B8E55B4DA5141035A2 **SHA256:** 7F5108045F455FFCAD1A4E4F3F0D77C35E2E80CDB170C6828B6CEB2A678B70DF	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\19a1b0829885d278_1 **MD5:** 7C6F24D95B8957DCBAC34BC029949499 **SHA256:** 8FD00EB23F7F5941961284F640C5F38C231A7E8AF54C60295FA8E687532A607D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\4d403953c4274313_0 **MD5:** 1E628966D5F4CDD1F23FA766E7061F67 **SHA256:** 445A56AB4CB9FA7ACC2ADA87BD2575743E13B08787060B7E87462A66CE39A48F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\95fcbb4ef0998598_0 **MD5:** 8FA726159B2E887FF379F92E15DDF7B2 **SHA256:** E9119167D67623ADB82867959E6B6B6F65F3B3232B30C2171E9791DA5C3DE476	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\34d467f947acad13_0 **MD5:** BFFEAFDFCDD2C915AC896FD7A586C55E **SHA256:** 3EE259F86D0BC6E4F886C37EDCBD7D7A1D2B006A3F84E91B2BF1CD47AFC71F7A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\b6a609a2a4d72ee3_0 **MD5:** E481646DD4D3030D658223575C1E897C **SHA256:** 3F13180C4CC24DE6700F229A140D983F25BB3FC6D4B6398B86E3278888733E68	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\5e44a7f4adb70c29_0 **MD5:** FFA59865F8733DFEF30D9F46F6308E3C **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\c95d30c9d70f69cd_0 **MD5:** A79F763E03522DA2BED91452D4F91885 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\4d403953c4274313_1 **MD5:** E80BA6C34E3D3854FF4976F16AA4BDB0 **SHA256:** F58A9B65133AA06D45078BF12F5E9BCD42713CA044508EAEC41DF05E55FED2F9	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\3881c13d201c7aa8_0 **MD5:** BE6882744F4805D455AFE1E90C607778 **SHA256:** CE6B65BD73C19F83ADA5CBC6CBFDECC63263C8DE0195797DCF99037FF732618C	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\b1eb612d97acde28_0 **MD5:** 6AD819F8ABEFB02E5AB22BD5CBD2D2B1 **SHA256:** 70EA17C3A4E0DC66EDF1358667F470A02E0FC6F278271106D3BEDAEF226D8875	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\a35caf37911ffc68_0 **MD5:** BDE04C5FF3AB20BCB1FAE8377CA56FF5 **SHA256:** 75E3848F1593AA1746A60C210464162929956B5BD33DC7E7FE65AEC107BF39B9	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\ab8e5be042409c8f_0 **MD5:** AB69668A93438EF46810FC8079311E33 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\7b242180316745f3_0 **MD5:** 167A2C0AE2FF28FF6781B88FDCD4C7A3 **SHA256:** 9BD4E94770E5462BD7CA297308215E21343584C7A8D20323563EAEABF3246E48	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\a674423cfbfd17cb_0 **MD5:** C6ADA16B28A021D174300197850609A7 **SHA256:** 4D06F7B43DC027E1A0D28CD375BDEF39E98AB7F653E534205E00EC652F69981B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\3b03edf631539a03_0 **MD5:** EDE38A1DD2D9843EE4E4FE84A4E10E28 **SHA256:** F83C586BCDBC07F0D5865682EADC26AED597BBFEFBEC1F77C8C4BBB243839DBA	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\22d4a57ac4e23ec3_0 **MD5:** B1C915AD16B9A812C54B7AD2504379AE **SHA256:** 7BE011447CFBC3DB032BD667DA8C87162119D4911AC408701745EEF65D25FE4F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\a4eeb911b4b433aa_0 **MD5:** 30CDF7085673130F24583AC39D7E14AA **SHA256:** A167E66AE91AC05ACDDA1E909BB8B985702B90D4D24712990C7D7F5E4F308437	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\f12d9bd42964b0e9_0 **MD5:** DB7E54AEAE1E6DF5CE7E1FEE61E5AFD2 **SHA256:** C7EBE7F9CA08E83FC98EFFEB13F3599DFDBBF1E664330F0F3C13EF6A98528E30	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\8c2129e90010758d_0 **MD5:** 58C99A36E36C1C45F3DD4F48D082E380 **SHA256:** FEE72F870623C754BD5442612299C413D0DCB3ED1459FC7677765E698843628F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\9e8aa4fdf814d5ed_0 **MD5:** 6C6D5C5C78EADAE519E762247D98AE4E **SHA256:** 1CB4D7CC9FA624AB078AA17CAEA05F4A2E31094C35B1ED17FF72F5C882E72E18	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\383a36fceaa62055_0 **MD5:** D0EEEE2910BFDC022098FBDEC75D8DB4 **SHA256:** CC8018651ECAADB21D1E4B37C07A89759A9A7565E6109D1815E10F7A1560C2EA	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\3baf6e1cdce96d35_0 **MD5:** 927450B533FA5D30AF1ED6F724D18E30 **SHA256:** 1189E1BB874C01E8877568E1B76744E01A3EEE3AFCAC55FE9BBBB144AE521F41	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\b4f84b300748a114_0 **MD5:** 2366963B85E5FA094D726B0DBDA36E1D **SHA256:** DC6B80B98C7F5F4A85062EAD4DA8F522EFF836A54E4EC4A3A07839C340676EB2	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\4fce287b5b441d74_0 **MD5:** 5EED51204479898D4E12BB0EAF6F2599 **SHA256:** B19E7969DFAD5133F14A7DED277E1502FA5B10B98AF7BF25A3DCC3FD5928E39E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\f1b076f89f1cca1b_0 **MD5:** 6982FF11BA015F51487EFAA39DA767F0 **SHA256:** AE30EDE78186B4C4D4C1EC4D7C0D7B814A207F2220BF4F12CFBFBC5B4C4E1CBA	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\5c14882e51891d25_0 **MD5:** CC66D7BECA02E762A9EE0C0B47E9FD89 **SHA256:** 68BB6CAC29F8307A07797A91322C8AF9B9AD7B7F7601F370F6924674389E6F8F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\79f151d882f08df2_0 **MD5:** DDBB9EE9A21BE7061BDA2F94A4F0CEC8 **SHA256:** 35ABF5D45956DB6651FB1AA6F3189769487936DFD1DDC976EC03DEF950E5C285	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF117c61.TMP **MD5:** 78BB216E06E8ACCCE662159FC222F6A4 **SHA256:** B287F620836469CE59FF80699F4EA19A783BF91A1967D8A3E824F3F959BE926A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\9c41141d-628c-4ca8-b7a3-6713bad4b716.tmp **MD5:** D341E6B7DA84C85228D0FEE7A312441E **SHA256:** A0F671C8AAB071F1CC264F57ED8D222543AA3E39EABE7EC38702544E76B3DE57	binary
8852	msiexec.exe	C:\Windows\Installer\117aab.msi **MD5:** 0378815D113388B4CDFBC1D20DFD46BF **SHA256:** B49B2C8A7846FB18709F3D2DF1062796F55BEC9C7B9674B7BBDF2108D3AAA68E	executable
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\10321e9873897921_0 **MD5:** C08D6306453AE858AEA8221101C31CD7 **SHA256:** A705B9187F56A49E181D950EA4852B885C95A12C6961B0A86CC35B707379D6BF	binary
8852	msiexec.exe	C:\Windows\Installer\MSI7CDE.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_e18e2bed1acda1b5_0_1 **MD5:** 9206FC369B170E18ED37998CC6E15991 **SHA256:** C1793510C744082055BB4C72B9CE473EE7B05E896BC17F0911ED72D4D79F3E7B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_46e0461e9e2474bc_0_1 **MD5:** D964942DF457164F7A7A8698146401CA **SHA256:** C7E4B06DAFFE689796260FA2AC99254793437971ED1AE1B54FC7FFF73AEC022C	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\6963dd94-8911-4801-8139-bdea9d022ad2.tmp **MD5:** 275481251FCA54F863D64D8385C0E65F **SHA256:** F815B8759D432BD710F55375226A8DC80564C60707D10F14EF361F534D1B1601	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_c879a3096bac60cb_0_1 **MD5:** EE11A1E35756BAF247D46BADC03E6B27 **SHA256:** 9F8C341A0DDDF2924268CE2C0C4CB8F529A2F8360A75C6BBB18EA3E8704303F5	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_c742a714249c2651_0_1 **MD5:** 8C28E118714AA3BF7C49EC753DF94EE6 **SHA256:** 5DCE4A12C85FBD21780C4250188AC26F94FD6AB988122B7A3AC3CA6DA59E995F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_9b20af41e6f28492_0_1 **MD5:** 9039091200E6198529CF7C3C3613810A **SHA256:** 0C3FED5F9772DE3ACAE8C00FD4D65B3BF3E0510A9FA2969B8D696E5DE9474061	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_44716b53e04f1cf3_0_1 **MD5:** FEAF33CF358192DFB5B79B4F9DDD7CAA **SHA256:** CF2ABE0784C108B8DC94978C64228DDA2011F366EE22057F279AA0B687B0A757	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_74e3b29b6a45b532_0_1 **MD5:** 3C1427CD9B54CBD82A1453B134B2301E **SHA256:** 12694A8E901E12C820197ABC26FE0AB14A6345198B60FAF625A588AE0B6D79BB	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_cb8f4134931fd007_0_1 **MD5:** 0A4E4E79EE355A5DD135B042E9AB28A2 **SHA256:** D7CF78E1448EF6C36F9E2A26F31D2B2091B852440F60530E1D55BAAA248E2F17	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_db1046a770baf17a_0_1 **MD5:** 2337B06B9D2CE2751ACA33D520F143E9 **SHA256:** C06EF9DBCC995D07F4A0B39734B74DC552814128263430A12976C440813153E6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_61acc149be17538f_0_1 **MD5:** 0C3D5C1FC9738805300B509BB3A188B7 **SHA256:** 901407132A76558A3FF23C2F73871CABE56C3E1FC9D5C7565DEE3E1BBDC7AB9E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF117c9f.TMP **MD5:** E1176CA688A2F72CBD1F60A5D075A706 **SHA256:** 589BCE0F7B8DC7F1A3451BD891251E7945B599C03473182F5040DF31FD2DA184	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_e9fe772137ebb7c9_0_1 **MD5:** 3922178D94ED3FF7547287B1A1760AC2 **SHA256:** B7BFD1302663029F254AAC22A6197A31CA65600485E8931988BCC2CE27014F6B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_80fbd7d5f3daf1ad_0_1 **MD5:** FE6A95D62B6175A4AF18A84EF065E40A **SHA256:** 5BA63D359A952AB176B0BC048B76827009C513B0EF7D4452187722BBBCBC1A8A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_dfb7c4486cc213ed_0_1 **MD5:** 87CDF98CFE48388F133FE26F344D9B29 **SHA256:** E0DF9BF19898E17D40858265D52C3867398FB93F88B0CDF2342ACB7351935C0B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8e5c720a5424291f_0_1 **MD5:** 0EB07504D30436E08A0900B8661C619C **SHA256:** AAA2EE6069FDC1FF48CC0C2421ABCDA58F542097D57AEFA733C2E34DC6090460	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_44716b53e04f1cf3_1_1 **MD5:** 86332B7EC752574F8428615F3ABF6422 **SHA256:** A4CDE907BCDF6773131115FAF59358F2E4C3006BD7657B257DE593990DDD1353	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_e18e2bed1acda1b5_1_1 **MD5:** 265B0C087AF2EC5F74F4B2C91C1627B5 **SHA256:** ED30D41DFE42378480B0A6892E27768D700CD33E12CC11BB0E5257687745FC05	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_159cc16c455920a4_0_1 **MD5:** 4B0B98AB1C7C4FCDAE068F255142178B **SHA256:** 6F87575648BF811310EE8F5182ADF3D88007AE49AE6A0F637C8F681E0FF059AE	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8f5f32485ea3157f_0_1 **MD5:** 265ED69FD42FE3AC7225BE3F5BB4C0D6 **SHA256:** D9BCB4FFCF77697EF0ECCA073310CC2DF985EA7E88996A0EEBFFDBA2A9C70924	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_159cc16c455920a4_1_1 **MD5:** 1F252367F04454531491A45CF719AA49 **SHA256:** 7092B9B613ACAECDCBB918E0DF68A57D6BC11DE4167A84773AF9470BCB1BF2DF	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_cb8f4134931fd007_1_1 **MD5:** 5CA8D419DBD97DC9E8DD59CD13581843 **SHA256:** 6DCA48B06A784DE366D045954631569BF8BA34B89248AEE93A1D750A15F15C53	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_db1046a770baf17a_1_1 **MD5:** A6D891D7081918BED898E79E3DAE3B51 **SHA256:** 6990A4F5FE1E9C8FCA9F828DE898E9F34516899E84EF23D3CCB00415C78954FD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_c742a714249c2651_1_1 **MD5:** 22FCFCA3D55CCAAFE7AAD785F3987AFF **SHA256:** 6A75B75994D22CE4955314D09B181130B275885A23F575865B8FEF7F21D7439B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_61acc149be17538f_1_1 **MD5:** 635A6E343721E90688F1F786DF18AF3F **SHA256:** 5F8B58B5656E20FE5F1EEBDEE53AF2861C44D3FBE500AEE37F31E8C293DC3840	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_74e3b29b6a45b532_1_1	binary

PID	Process	Filename	Type
		MD5: 520FC857FDB8753C4A963F3CFB7FACC0 **SHA256:** 215D6C16F3991D47441F6465CA496E8BDAD0502B4F1EF5D6699DFA2A21C24CB2	
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_9b20af41e6f28492_1_1 **MD5:** 8D37D00E9875373125886ED0C1DDE451 **SHA256:** 4D27B685D755298C55ACE8F3BC543B5B861A4363741E5D3F9B096E8A4BC32745	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_80fbd7d5f3daf1ad_1_1 **MD5:** ABAE2636C48F050570AC7152DBB9A3F3 **SHA256:** F8860AAEE64A190984313FF0AF76EAAC51FA275387BA32413D00F7C8211FD3A6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_e9fe772137ebb7c9_1_1 **MD5:** DBE2E19B97DFAF9B42AB288FBE8F4DE8 **SHA256:** 3B4F3EEAA5611118C72C24C185B3D943E19BCD9C60F296D51EE8D45A2739B8FE	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_dfb7c4486cc213ed_1_1 **MD5:** 0E6C90FD9058441ACADB479BF439E0DC **SHA256:** 5EFFA76FCAD6DF5367136341D821EE6600DD54109C91D33EEB92BF3D68DD5F28	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8e5c720a5424291f_1_1 **MD5:** D899CBA0599910F86E3BA33FF33B1438 **SHA256:** 1ABCE4045F99F50FD4BB7C592FA936F68AA380C9F6794AD7269BAB3FCA812FBD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_c879a3096bac60cb_1_1 **MD5:** 3CF4E799443F03A81AEC789EE62D8AD9 **SHA256:** E26B36AC07E26FDA434FC115DDCBC54DFE17EBCE58452ACAE7600758AAEBA28D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_26e54f7d739c2e8d_0_1 **MD5:** 24F0E67982652C34D15557FE2FCB9545 **SHA256:** F738DDA00D7D7313028C355502585DC9F4D164D6A3CF375D3B81165FC85D5123	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_b2999b4b79d0395b_0_1 **MD5:** D06F7C00F78FF43D0A39FC913F0D6BB8 **SHA256:** 154E1A370E155DE078F09D3D8BB3EFD1124E58F5B033B58A8805A5C89C25737F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_27416bca4f53f522_0_1 **MD5:** AEE28E8829D06D1A625D97A8D02C238D **SHA256:** 144B1D60AF8A44ED50DEE18C7DF6A145D8B59EC147B94BCF4120FFA0A21FEF88	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_b2999b4b79d0395b_1_1 **MD5:** 2DBB76D798102C79A666756348B03921 **SHA256:** D7EAC10AB8768C345EEB73A4A7228E3F594B1927757A769557B83B82AD11275D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8f5f32485ea3157f_1_1 **MD5:** 09A05970B53CA41C1779367845CAD4B8 **SHA256:** 9F49DA50BFC9FA568D373A2AAFFF2492AC71AD548837B69C548804B9F5932161	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_14e14362a64d3c02_0_1 **MD5:** E0226E156732AF0D69F14C3F806321A6 **SHA256:** 4191B78244077F06673FA6D8F710939EC759119D13DFDC54EFBAB6BA9BF1D60B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_04e0e24d3bac9498_0_1 **MD5:** 93D7EAFA58723F84BC062AB41030CCBC **SHA256:** 82E689F7CC81366E4E8A297864A78066B98ADB4358700624F3F83B9242BF3AA7	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_ec37128008082892_0_1 **MD5:** D52252E88C086C00E820B781527E6465 **SHA256:** A47C9DF4088A3DCDD4CDC20A5AF104F0754D9E892FF406EE2CC10632BAB38F45	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_28508364fc90be9d_0_1 **MD5:** A87069BB620EF6258AA2DB7849F62D4A **SHA256:** E928DECE95A784B57518CB4B353BE441499C2A67DE55DAD13650ABBCEF8A0B68	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8ec601edd4ab443e_0_1 **MD5:** E09B6B5F69A903FE9F284E2CD531B646 **SHA256:** 12DF0082C820B7AB64A93559D29585DD521630C88739AFA3F08B3A6B4FDFD88B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_577f937d5a0ac9c2_0_1 **MD5:** EEE1017917D20498AC059F581C346872 **SHA256:** 8FEFE8D21D29E290BDF6B3DC459E12C0F9CC5107CB3C867A86CAD498CE38A6F6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_06dba16f38ad96cd_0_1 **MD5:** E3E09778E4270942A39A5890FB809B7D **SHA256:** 1533957CAC5E1B921E7A8FB19B746C979B8EC52757E0B294660FC79F40DCA167	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_df951115239b63a3_0_1 **MD5:** 40D4F48B352AA418073B39BEA701A87A **SHA256:** 45D081103C614332FEC85030D08597B495AC6F935DED36863FA33FC76EF08EFF	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8ae450533bd52451_0_1 **MD5:** C9B487BB3DA50FB5CE7AB0A58A9831AA **SHA256:** 3DA28F7DC6ABDCD4EB579F14DA0E0E133A32BBFB3CD6F5E8D60BE249FB2ABFAD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_3f748e0ccf479d55_0_1 **MD5:** DF81649369526342DF9F8C07E61960A1 **SHA256:** 86D18DE5EBD6B68A090537FB98C712DEA5395626EF6C362783F1267ECABC3F87	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_c6c8dac494b31915_0_1 **MD5:** 708FB577CF9979D4BFC17977BF8339D2 **SHA256:** 23A66BD2234D87A76D2153BE83F2B7D57DAE0590278DC2C82A824BE21416A3E6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_bb123c2e42c43b94_0_1 **MD5:** 22E245AB2D792CB2855661BEC31A59CC **SHA256:** 574BF08239C8498D685CE0E76A80962BB418F103EF4865054BC2745F6462DC31	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_27416bca4f53f522_1_1 **MD5:** A3EA1243581444C872B694DF060D71AF **SHA256:** 921207B1096670011D6552D0A77FF0043D063FF4CCD2BBA721A967383C33774B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_26e54f7d739c2e8d_1_1 **MD5:** 914299CE431B0AABA791EB80B1D1E000 **SHA256:** C0D67B3F38A5F67C12D6F8B4444B262C2B96D3C0272963780CEB1FB80ECA3B0B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_99bfaadd50a2e551_0_1 **MD5:** F904ECAEE465060458678C3329C2F01D **SHA256:** 0833BB354A19094922496847DB7255A17763C26EA600340B7AED42B1261A3222	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_c6c8dac494b31915_1_1 **MD5:** 8BB87D1B99EF8CA1A4524CEF732677EF **SHA256:** 831AFCDF4661CF0CD6BECE949862E7A537E93AB10A4165363B01BA3CFD758517	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_04e0e24d3bac9498_1_1 **MD5:** 20E2C6C62F82E7385BBF115061DDF08C **SHA256:** 80B3561CE6F5C30F870356720E0909751B194C8701179F9DEABC94436C0FBC38	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8ae450533bd52451_1_1 **MD5:** 97CFB5632CAEB3993C6FF2D05312ACD4 **SHA256:** 38758617E36D2AE3F7F02041E429CAF24CF476ECD62F761858645F2D75228F6F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_14e14362a64d3c02_1_1 **MD5:** C3F1B96DB9C824E2F9F5E36356DFA5AC **SHA256:** 6C858B2948251985B00FB2CA4A6E64E65930D911D9A63F331C27531E85C3A7C3	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_99bfaadd50a2e551_1_1 **MD5:** 512EE11D37C62BA311D081B33B03C8A0 **SHA256:** 80F905E47AF04D6F3E93F4BE69F326F436EEE47686F1B8C9B5B14612A37A7BA6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_ec37128008082892_1_1 **MD5:** CCE81D79764CC78DB6D505FA1857A18E **SHA256:** 3A2EFBB65C4981861D5C44C782D1628EF3F52351D9E1B5E9050AB523403E1822	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_df951115239b63a3_1_1 **MD5:** E2C2F0FCC8C2AAB3BF52EDF790920BC6 **SHA256:** E27EBDE808593E32DACD830ABFE5D310DB8CC6C4F63CC7256CD7B2E8CEB72042	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_28508364fc90be9d_1_1 **MD5:** 7CCB66C821E265D424BD2BF4DE09CB48 **SHA256:** BB098BBF50C77AF496E59D74ADC0F3A43AF5790E9AD9239FBE232630FBA749D0	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_3f748e0ccf479d55_1_1 **MD5:** 523AE2AF525B72A39066970BFE76D5E9 **SHA256:** 468FD4FB30204756442A2E228B117EFBEC7871A431302514D03977724A36D174	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_06dba16f38ad96cd_1_1 **MD5:** 5C6A9DCD64E4A80CC884BB71708D712F **SHA256:** FB6B54049C931E97E6447192F5561F34A34C6EDE81F44F53F7DFA36F48C56DB3	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_bb123c2e42c43b94_1_1 **MD5:** 68F533D4425FA66B168DE456782CCE03 **SHA256:** D1CE87EF16BD02412868C112189413EEDDAE9784026B8A839FBB9FF685D13CDD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_577f937d5a0ac9c2_1_1 **MD5:** BBFBA918A485BCFC3B81A6F8047D2BC0 **SHA256:** B6EDC67AFD4A6228913FF9EE3CF5718B2E24FD834FA2950F2627AC019A15252A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8ec601edd4ab443e_1_1 **MD5:** B8440E8B8F840412492D891D7B5C22B7 **SHA256:** 88F0291F5788C6697D1A7E4AA8F3890E10ADB9E4BC3696B5A5C2D4885A2ECBC7	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\352d3033-3d1d-4bf1-9db4-c165b4c172de.tmp **MD5:** C119B92344A4F263BAF43E5C5C85CC40 **SHA256:** 556AFE9D95D303B496AF03D042675520B10421F0F1CEA79DD46CD78536CEC592	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_c9446ec985cdd6dd_0_1 **MD5:** F71DB6A7108392B9D0D04BECFEFB9447 **SHA256:** 261D0AB717A88B2D1CA230D1BA23FE0CC3F344655ADE43121658A7CCB49368BE	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_d46f70378d57560c_0_1 **MD5:** 23898EAFC1EB12A9D148B959CE9BD134 **SHA256:** 4B5176906F5C26E2D0E44234E95E574548E82EDDA4B2A4BFEBA95533840993F8	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RF117f2f.TMP **MD5:** 7E8EFAB591A7794E224ADC063AB89622 **SHA256:** 59015A92ED553AD9EDD4F7C618DCD5751462C996E6016BD6DC811E5B55BE1091	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_a5be65a9c78dea4d_0_1 **MD5:** 9AB98883BE48F77B626653188CE83350 **SHA256:** 4A7E05ADA5CF041B15450B2B43DFA53AA4F74E1F9A482195B86C2B17D615D2D0	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_c9446ec985cdd6dd_1_1 **MD5:** 7F224A5FF8B9E83B6564A8EBCED5B965 **SHA256:** 75047894EF23BC048B5D4C7A1967F0890664F4BA41185EDCE50FBA7B0BA1D255	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_f2b9245231fc1f18_0_1 **MD5:** BD075B7B65D6738181C329837449DE83 **SHA256:** 3D17D4921F4ECCDA1A16A62FBE27D945EB4CF755E273AFC144C7C1E5DBC3CBF6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_f2b9245231fc1f18_1_1	binary

PID	Process	Filename	Type
		MD5: FC994580874A39846B21C6C7B089CCC6 **SHA256:** A832FB2B6FE9F329E6CF33228BA81818EE42D1FCE5934EB4DE7474DE9938A6E5	
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_d46f70378d57560c_1_1 **MD5:** 89A6C6DDDD0ED3BFE2177C8C486352D7 **SHA256:** 49812CDCEE663CD9439D4B29C684AE7505A33AFA831F9E23EA108704560AFA42	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_0daf6f81a068aab1_0_1 **MD5:** 41D97B71852F58F2E78317061FB346C9 **SHA256:** 8EF6FF9744B63D7682B1ED22CA0F67E2B8F152BB00BCF632983B00D863EBC1BB	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_dde6b50ba3e3e7d9_0_1 **MD5:** FCDAF24CA67E0D0666110F2DD6711894 **SHA256:** 6A40138F29B9D2592DADAC4DFC81AC2AA4D13EFE5C0C02D6CEDDC67CDE064469	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_a5be65a9c78dea4d_1_1 **MD5:** 9D697CA59231FA0D799607E3BCF73872 **SHA256:** E3C5352B369202D91CB1839A61B386EE1BD1F0E0A7900B3396AE92BC870B03C2	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_958fb52153fdd2b3_0_1 **MD5:** A034710C8132B39E65398FDC34AC852E **SHA256:** 3E9F5096CAEEC52D7E358F3E5EFCE6B9267CC38BA4EC2776A0FA6B67EBF01441	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_aa825a1bc344923e_0_1 **MD5:** 063E94F2BA8282A7A8807DF0A7E73CAF **SHA256:** A85A3AFA416EAD1655A5FEC06BC760CE9495969A7F7E35EBDF32F8F9202C99EA	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_04ca4656472917ad_0_1 **MD5:** AD06662C24B6D178837ABE1DFD85BB21 **SHA256:** BC9A4A7DE6777990D01B6E3CCC224FC5EE0E5D799454F59E045E0358F4DE8E49	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_6836b6d12d369b00_0_1 **MD5:** 7C30DE826F6EA5AD70F19CFF2BE3E98B **SHA256:** 835131FE50DE07D2953C1BAB7AF8544FFC2F58285F27E4F397B25A8A27FAFF18	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8bdfcf4ddbb4a3a7_0_1 **MD5:** 625CAB250ECB507381C3B2099DA0C63C **SHA256:** 1962C09422DC1AA88DCAD6B16A02FED3E9432E459F06A4F10F6081AD24A8ED1A	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_0daf6f81a068aab1_1_1 **MD5:** 471EF81FA79B7C24ADEBF45EF8BB74BF **SHA256:** 5B33681AF7F92C957510A093EF94E132BE6F8DB36DC40615FE1D43BFB0FC3059	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_aa825a1bc344923e_1_1 **MD5:** 929880D1110A4743F1D9470E65F85A7D **SHA256:** 48E0229292E15EE0D79E7E8FC18B3837969839075BC1519B8373832FACB40742	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_27e74e20268bdeff_0_1 **MD5:** B693A30F5B63F9E327DFB4AC8F1BEA15 **SHA256:** 6AC2A4E61046653454920 3FAAE07CFCF87FF1C5B9F8D0AAF34D5F7E4B9C402AC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_8bdfcf4ddbb4a3a7_1_1 **MD5:** 944A5719C33853CAEC64EA71908E0201 **SHA256:** 746FC2C2866C6A083BC8298294F6C1AB8418B97E668505BB7B5419D181966656	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_dde6b50ba3e3e7d9_1_1 **MD5:** 4E23523108DDB30AB5593EE608979079 **SHA256:** B35F257F0F12EAD70D51BACB56D3D392E09B00E81D38CC98DE8FA57AE88554C6	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_958fb52153fdd2b3_1_1 **MD5:** 8DB88CB16B156CFA5657FFBAD0FF0934 **SHA256:** B5BE76F46758574EB4E42B0DEBCB97053E8C4F9CBDE1535A15FA35BE00988439	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_04ca4656472917ad_1_1 **MD5:** 65A9BB19FF6DA512682137D149261ED0 **SHA256:** 8DB3001DA6E0CA864FB86B2EA550F87C98801DA5BACC336BF7F86ACFCB1B5750	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_6836b6d12d369b00_1_1 **MD5:** 9C4A967AF2C47FF8B58CD24821B4F50B **SHA256:** 3F0C1941A934261FAB0CFA5129D5C4B465258E93769DEDAD098D00D87392EB9E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\IndexedDB\https_ntp.msn.com_0.indexeddb.leveldb \LOG.old~RF117fac.TMP **MD5:** 0825EBBC01C197BB5B336E831FD36F4B **SHA256:** A49FE56A5A4AC6EB696E78EFC5BB59E7C78EFF54EFF8CE48482020F72B4D10FF	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\2de1d2dd-b02b-4dcc-a032-9547e0b92627\170ce29fd1bcbf73_0 **MD5:** 0F20A2E013DF17B203B17BC2F3424854 **SHA256:** 2C23D66E6E126BC5D63F100EA0E6B546421953AB0998650E599E7696863C33BD	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\3095802301361ac7_0 **MD5:** 20282E433FADC506A47B7BEAD0F3D151 **SHA256:** 2DCD57D365AEEB8BEF5FA73ACD814A53B6D9A4C551EA41F65AA441ED4EB3BC3B	binary
8852	msiexec.exe	C:\Windows\Installer\MSI7FDC.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage \3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\todelete_27e74e20268bdeff_1_1 **MD5:** A7E544FF5F6F5EC540256BF7C429B9B7 **SHA256:** 56EF6066F4097F9C8CFFA13C544F561A25CD7A40EA3C92FD11FEF79E0E285C67	binary
8852	msiexec.exe	C:\Windows\Installer\MSI804B.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\5dbf58d00576287c_0	binary

PID	Process	Filename	Type
		MD5: 018345762C6C9566F50D1B6F8AED8C0B **SHA256:** C04F49BC03244EE8121024F3B87A4D2CF217E6696E1C598703343A8967224EB1	
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\5038f55110c4aad7_0 **MD5:** 0490974F9AFFEF40DDDBD51BD392DA1E **SHA256:** AE4F62BCF26D80254AD0BC921E5C976C65E1D81DCA9B3C773443DAE332272587	binary
8852	msiexec.exe	C:\Windows\Installer\MSI8195.tmp **MD5:** 748B2602C9F9884DD718B958622F033B **SHA256:** 7F6BD90D567D13C53DA8FE4944A4496E0A68AC55CA74661C51A1609034B7F302	executable
8852	msiexec.exe	C:\Windows\Installer\MSI8155.tmp **MD5:** 2471A6617D7CF84A1E56FEBAEC7BBBD4 **SHA256:** EE716592A3A5919DFA625AAB252C4EFD0D03066670FA0E28082886B4FD226950	binary
8852	msiexec.exe	C:\Windows\Installer\inprogressinstallinfo.ipi **MD5:** C2849E3F8BB77902F631D90BD970D232 **SHA256:** FA4906B3C31BEE085DEC52C7FD39A237150BE53F73BAF6C94AF7BC384E693540	binary
8852	msiexec.exe	C:\Windows\Temp\~DF73138405123E982E.TMP **MD5:** C2849E3F8BB77902F631D90BD970D232 **SHA256:** —	binary
8852	msiexec.exe	C:\Windows\Installer\MSI8271.tmp **MD5:** 748B2602C9F9884DD718B958622F033B **SHA256:** 7F6BD90D567D13C53DA8FE4944A4496E0A68AC55CA74661C51A1609034B7F302	executable
8852	msiexec.exe	C:\Windows\Temp\~DF7663F541FB8E7C4A.TMP **MD5:** BF619EAC0CDF3F68D496EA9344137E8B **SHA256:** 076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\824965b1-8af2-475b-a607-c7bcabbb5bd9\todelete_e30082db9c6a6650_0_1 **MD5:** DB916644E322BCCDAC75867840DE0386 **SHA256:** 0B3A54958DDF86390B5338AA4BF2F881BEF49FFDAEAC13FB019BF121FAFC6C89	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\824965b1-8af2-475b-a607-c7bcabbb5bd9\63f50aa2cd372d3d_0 **MD5:** B4D556DCCF3FD5614E884ACA82B454AB **SHA256:** 88E457D8D1E5A6509727F49A3302B68A6CDDB93B9405B08845D5D1C90B3BAFAE	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\824965b1-8af2-475b-a607-c7bcabbb5bd9\todelete_26ba3991c57e2fa0_0_1 **MD5:** B07D70CEEF59B5FF275DA78743C94098 **SHA256:** 398CECFCD555EA47C7A85422643FD00DE6870E0E180850AAE2F7D3D32C376E02	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002cd **MD5:** 127E39F43DFB3411A5CA73C8232847E3 **SHA256:** D5A497D42B451079985158EF5E3F7F198E5B5D55A0BDE95C85863964905B381A	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002cb **MD5:** 39AB8949071AF3340CE5DC6AA07B312A **SHA256:** E06DAB06B1EB73D172727A6748649FBC7CE1CA084662563ED61F8947CCDFA808	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002cc **MD5:** A507BA29074F7C6BD4E097F8DF3DD4CB **SHA256:** D4AF1F05EA60468650DBCD04F375677B7F0A8F01AEB917D03DF26F973991019E	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002ca **MD5:** 3668E5ABBF8164C374D4AB9AE57D9D8F **SHA256:** BE2FBC8768236D013AF641E2BA939F10807375ED98FB3F987CB5A6730A668A6E	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002d0 **MD5:** B8EBB4F2FB4751F8F02FB8E38AC2806B **SHA256:** —	image
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\aa097de75cb95560_0 **MD5:** 17E33B53F2FF935AF02DB538683DD38D **SHA256:** 83FAA27C5D15A1B537B897C6879E044753A7CE4C4D79E68DE3AC5D5E2A10C5F6	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002d2 **MD5:** 1F28D7FB9923DDEFBA923303D3F23CE8 **SHA256:** 4724F96791F6380F9227AA70323BA925CDEAA85C79FA2B04DAAD0CEEFBEAD33C	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002ce **MD5:** 4521358075BAFBBB10D8218F547D12F9 **SHA256:** 7E2900F73E28955DD80BB15892C27C3DF8421382D274438AB7629D5ECF56E54D	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002d1 **MD5:** CD71661A87B5386B85A525FBC957FA9C **SHA256:** 9E0917EAFAA6202A26013465E47F113AA916F26A7DEDC55A86AE6E7FD7C0698E	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002cf **MD5:** 0DB1A7BDC6E3D1589296956294851627 **SHA256:** C01B0DB277AD93829BA3F886B55B9B44FFE2A8947C8A3EC39C3A7A7F77966D76	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002d4 **MD5:** AD8A570AC09B72BAF2555BD8581FB651 **SHA256:** 916B4E3DA9B4FF79EB83C3967EE357F307536F2AB526124F3E610651D2508194	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002d3 **MD5:** 7F378471B6829700FA2E6BF11470556A **SHA256:** 892E02D3745B8C61FDD6D89AB786CFDAE6FA3B49DBC4DF3CE0D044C5BCB1D101	image
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002c9 **MD5:** 5A23EDB565C6F98A597154EC6C84B6D4 **SHA256:** 5BF13685AA5347F45DBCDCDE0278172554EB396F23970310D798C0C2B3856760	compressed
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\7f0a0841d1bb68c5_0 **MD5:** E86D72CE37C09D9FD353F9560B0A7E28 **SHA256:** 19A20EFEA4F0A2A9690AAF748897116776FE234DD3A6AA8146EF327D4AA04F73	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\08993a70f5dcf7cf_0 **MD5:** 415626F85EC8B68691A11EBC2956793A **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_0002d5 **MD5:** 311F1298863858C8334BD7A8A0E34014 **SHA256:** 846351F83ED17838A1DE223EAD4E9900D1E127B3243695DAF5A4988E965C44CC	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\DualEngine\SiteList-Consumer.json~RF11a11f.TMP **MD5:** 0E3F8C96A0348BB1C7A94E3DA2B68BF0 **SHA256:** 8232C450F967D7F2F22C54582F0667F4C033AE62E6D450FF8A35C47486249443	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\DualEngine\SiteList-Consumer.json **MD5:** 0E3F8C96A0348BB1C7A94E3DA2B68BF0 **SHA256:** 8232C450F967D7F2F22C54582F0667F4C033AE62E6D450FF8A35C47486249443	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\DualEngine\3832913a-acba-4611-876d-5c02b94b7195.tmp **MD5:** 0E3F8C96A0348BB1C7A94E3DA2B68BF0 **SHA256:** 8232C450F967D7F2F22C54582F0667F4C033AE62E6D450FF8A35C47486249443	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\4112638a-b1c4-4315-804d-449d82e0f798.tmp **MD5:** CBEBE8793604C47BD9E38F086DFD5680 **SHA256:** 5CA1F13CF43BAF93669F79568C579956929E8A2D530FBC4D43D49205454241F3	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\cac25b82-319f-4086-a132-1199b2421017.tmp **MD5:** 082284194D1BCA5944F53EC4AC1F1DE3 **SHA256:** E95FB7AED6E1C604FCE06BCB87927156F482C1BD60A2668CD5ADAD4367CBC0CC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\index-dir\temp-index **MD5:** 0FB5DA61467B226A2805B8911687596D **SHA256:** F55E8EC087077D91AA8A1BA1A0F8AE15DDF75C0D435CDBD6DC95A1B07E77351D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index~RF11c263.TMP **MD5:** E2EB52E70DF1C99E623BF82AB5EE4EF1 **SHA256:** 8D6DF087DECAB19CE84DDF96A3AF01D713C6A2A2045313B039D448DD116101F8	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RF11a42c.TMP **MD5:** C119B92344A4F263BAF43E5C5C85CC40 **SHA256:** 556AFE9D95D303B496AF03D042675520B10421F0F1CEA79DD46CD78536CEC592	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index **MD5:** 0FB5DA61467B226A2805B8911687596D **SHA256:** F55E8EC087077D91AA8A1BA1A0F8AE15DDF75C0D435CDBD6DC95A1B07E77351D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\1be6528b-b619-4a96-b04b-1874aa44d255\index-dir\the-real-index~RF11b88f.TMP **MD5:** AFE30749F01C905A7992F9F465BA4190 **SHA256:** 4C073E45FB85D81AC9E79BCDC1E6B0A1E5CD732241EE74283728498BED25ADE7	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF11a3fd.TMP **MD5:** 275481251FCA54F863D64D8385C0E65F **SHA256:** F815B8759D432BD710F55375226A8DC80564C60707D10F14EF361F534D1B1601	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State~RF11ca13.TMP **MD5:** C52DF64918E1FF7FD33C01CBE58342ED **SHA256:** F880EC98D17DA1D0FA9603CBBD969A97C60511264BAFE0A063E2CBABED45085D	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1008306808\manifest.fingerprint **MD5:** 3FB5233616491DF0EC229BA9F42EFDB8 **SHA256:** 946F3A9E019B0D80F5671DE782F295132341F663F74AEBAD7628F22E528D6D52	text
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\b3e1a5e7-c051-4460-9485-8eb4431d4244.tmp **MD5:** B4226B1CDAC90D8757EAC0B2849CA12B **SHA256:** FD1B98064191D407A4B5E8C4696B353AF63304E26095B2DE9762FF4AA216A144	binary
2332	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_1008306808\manifest.json **MD5:** AF3A9104CA46F35BB5F6123D89C25966 **SHA256:** 81BD82AC27612A58BE30A72DD8956B13F883E32FFB54A58076BD6A42B8AFAEEA	binary
8948	msiexec.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\onestart_installer.exe.part **MD5:** — **SHA256:** —	—
8948	msiexec.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\onestart_installer.exe **MD5:** — **SHA256:** —	—
9076	onestart_installer.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\ONESTART.PACKED.7Z **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\7684a342-8740-44b1-84db-8c8bf45d81e0.tmp **MD5:** 215EDD897EA86F83B8C06AFD53BCF323 **SHA256:** 8CEC4271E884E2F1D12B658901A4D9AFB4784824A767C4451C287E24BCDC57B3	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\index-dir\temp-index **MD5:** 4CB76D17BCD2C3BCB3225C106EEA64E7 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF11c437.TMP **MD5:** D341E6B7DA84C85228D0FEE7A312441E **SHA256:** —	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State **MD5:** B4226B1CDAC90D8757EAC0B2849CA12B **SHA256:** FD1B98064191D407A4B5E8C4696B353AF63304E26095B2DE9762FF4AA216A144	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\index-dir\the-real-index **MD5:** 4CB76D17BCD2C3BCB3225C106EEA64E7 **SHA256:** C689BD9F3D2C94E5AC8E954B86A37E114B2B93C72180528864C255F4E2BAE183	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\2de1d2dd-b02b-4dcc-a032-9547e0b92627\index-dir\the-real-index~RF11ce0b.TMP **MD5:** E4EB6FBC5E151A8CAF5DE88C963A2A80 **SHA256:** 7978A842EDFFD58E00A85C357D103E64CADAE64CB9812B501C4F9B9D69A47DFC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\5a6d52bc-1d35-49b9-aaad-e1be48285a34\index-dir\the-real-index~RF11cdbd.TMP **MD5:** 6326976065E3A5BC720D536FAA0879F9 **SHA256:** 7186173AF228EEC2C437ABDE76D217D04394F388A7F7FB56C7B57159DCF563CF	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\824965b1-8af2-475b-a607-c7bcabbb5bd9\index-dir\the-real-index~RF11d435.TMP **MD5:** 1D12FF9627A6BF1CF3ABFE40CB087864 **SHA256:** A112316EDAB373FB2238D83C6ECD6A9E992500EF62B0A413DC6130D8BE672141	binary

PID	Process	Filename	Type
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\index.txt~RF11d464.TMP **MD5:** 6C87EFF947A7AADE723820D357C7395C **SHA256:** 70238E4337F5D88ECC1B30AF1F7AB9D5713D08679BE8B5912CF0C34B24B81DB8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics-spare.pma **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\824965b1-8af2-475b-a607-c7bcabbb5bd9\index-dir\temp-index **MD5:** 2C6793DA46E4049C8100319111CDC496 **SHA256:** 53E3B24390D214CBEF22781530B7BF8B475D9434D44779FF94FEAE30AD322712	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\824965b1-8af2-475b-a607-c7bcabbb5bd9\index-dir\the-real-index **MD5:** 2C6793DA46E4049C8100319111CDC496 **SHA256:** —	binary
8852	msiexec.exe	C:\Config.Msi\117aac.rbs **MD5:** B0536CA6E9C0E16EE360FBF8F4BCC0B5 **SHA256:** —	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index~RF11def3.TMP **MD5:** 981BB633E8D5E365E149493C3A31A8E8 **SHA256:** D33C86F66A95671CD2AED6C552DE62B13EB9A4A247A322AD5EC9B32B89E3CE6F	binary
9076	onestart_installer.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\master_preferences **MD5:** 746E45D4BE2D95012AFF9A0716E811F6 **SHA256:** 5269F6E042E298253D298CBE4A10EFECE8276BF8058A679DD81A9FA6FE91C060	binary
9076	onestart_installer.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Update\transfer.dat **MD5:** 9BF31C7FF062936A96D3C8BD1F8F2FF3 **SHA256:** E629FA6598D732768F7C726B4B621285F9C3B85303900AA912017DB7617D8BDB	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\c3c264b6-cf96-4d58-9b62-9170cbfdfe9e.tmp **MD5:** 57DF67BCC36C5037B452CA4C41ECAC13 **SHA256:** —	binary
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Crashpad\settings.dat **MD5:** B01505F7336310B71AB7E0A91E0C83A8 **SHA256:** 764A552D801ED4988A58107B89DEEAE6A09341AEB831895E2450A3A2D63AA762	binary
9076	onestart_installer.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\.data\OneStart.json **MD5:** 2F1B9DBE74BA59EEA3BE3C3CAB207E73 **SHA256:** D259FC06E9F9FD9660D56B1F785819213A75856D2458EA5287638154E2B2E919	binary
9076	onestart_installer.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\setup.exe **MD5:** 58AD915B20BEB605B2CBEA6543E9FB13 **SHA256:** ADC91A852F40C8E94C6DB80AC5CBCE3E6CCCE76AF8CB4EADA15E13255FAD1AA5	executable
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\132.0.6834.116\Installer\onestart.7z **MD5:** — **SHA256:** —	—
9076	onestart_installer.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart Installer\CR_B0029.tmp\SETUP.EX_ **MD5:** 9CF6A5C2992767979342A1060C601592 **SHA256:** F218760D1A7753D09FBD8C446171E08B84F78099F4593A832CFC18D17B39A1F7	compressed
780	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_2052028847\kp_pinslist.pb **MD5:** 2D8BCB7C4B2DC669429BD40F7048F62A **SHA256:** 7A0866CDD7BD21B8B08D166EDB3F6ADF8C859B47988B9B3BA3F0EAAFABE10FF2	binary
780	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_2052028847\crs.pb **MD5:** 24A3775317D74CEEA8FBA6F0CFBCE562 **SHA256:** 192B206AD6F649F6C8767F6A3B11D9C5354710602BF0AEB4157EEA08D7461EF7	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF11eb76.TMP **MD5:** 215EDD897EA86F83B8C06AFD53BCF323 **SHA256:** 8CEC4271E884E2F1D12B658901A4D9AFB4784824A767C4451C287E24BCDC57B3	binary
780	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_2052028847\ct_config.pb **MD5:** 09B6469DE61DB3473BDFE04951F08529 **SHA256:** 1C435F4448DCF1784637FA9470546D12D7DB2420A11CF8B5D6343439DD401C60	binary
780	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_2052028847\manifest.json **MD5:** 2C2E90B63E0F7E54FFC271312A3D4490 **SHA256:** 72DBB7D6B647B664EF64B6A14771C2549C979B9C57712F3F712966EDB02D7B2E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_2052028847\manifest.fingerprint **MD5:** 7D65B590511ABCBE48AD58E49B9A7263 **SHA256:** 71400B86A340E3D8F0048E2190E267DD38374995F47209F6C78E6A2D057BC280	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF1212f4.TMP **MD5:** 57DF67BCC36C5037B452CA4C41ECAC13 **SHA256:** C9AACAD0721534D4169E15907410707164CEB44B6CD947D920AD539E0BB80C41	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF1212f4.TMP **MD5:** 082284194D1BCA5944F53EC4AC1F1DE3 **SHA256:** E95FB7AED6E1C604FCE06BCB87927156F482C1BD60A2668CD5ADAD4367CBC0CC	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\4e4da492-3636-46c6-961e-c0983ea7b8f1.tmp **MD5:** FE86F804921307EA5BE22FC8424AE066 **SHA256:** 9361639248DD652E2B6489DFFA4E053ED63419D66DD78A3614F9641ABD2F3FB5	binary
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\Resources\icon1.ico **MD5:** 243528346024C4CCD98E6880C909CD55 **SHA256:** B5EA119CBF41A35A1B601517AF26202B4E22442D8B217FCC08B8414E8AE50FAC	image
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\132.0.6834.116\Installer\setup.exe **MD5:** 58AD915B20BEB605B2CBEA6543E9FB13 **SHA256:** ADC91A852F40C8E94C6DB80AC5CBCE3E6CCCE76AF8CB4EADA15E13255FAD1AA5	executable
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\Resources\icon2.ico **MD5:** 38FEDBAE1961CC5F2FD9C2D004AB76A2 **SHA256:** 9687CDD66A3D17D43DE85D6D6617C86FC6E82341D2451D53023138AC227F1122	image
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\onestart.exe	executable

PID	Process	Filename	Type
		MD5: 7473ECF4A1CF4D271455034708DF09F1 **SHA256:** 8E4C2959518998791CAB87E660520197260DD8920B229962D50EF0301739CC37	
8648	setup.exe	C:\Users\admin\AppData\Local\Temp\chromium_installer.log **MD5:** D8FC658484511F8DEBE21024F9CBC5AF **SHA256:** 51FEA1436F01034D7656316F3B8D04B4D3CABC1538D4F94CDE1CF5663D9402E5	text
8648	setup.exe	C:\Users\admin\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\OneStart.lnk **MD5:** 99D7A04067EA9552EA9E983143F0F455 **SHA256:** 493CC21EE45BD4872EB4DC5F4E735512106458FB3A517078B7548F183461C8F3	binary
8648	setup.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\OneStart.lnk **MD5:** 75208EED5A6BB2BCE2FAEE4B1700B856 **SHA256:** A31A44D34FFDFF73E97F01AC821BAAA60D944DF43D2405D2B3FBDEC4F39E5701	binary
8648	setup.exe	C:\Users\admin\Desktop\OneStart.lnk **MD5:** 695C9A492A4CA2BB993AE4B8A12E13B3 **SHA256:** 1B74B27844C70308FCF517607E14E8E9CDEA165EE5BA584CD41FEC51FC2DA4E7	binary
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\chrome.VisualElementsManifest.xml **MD5:** 2E6DD0FB1979F75BDD8F9B8B0E069D9B **SHA256:** 9BADFCA9F104D331B03C9AECC02A1FD0FB25E0F3572A9B4D678BB747B88E342A	text
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Temp\source7740_54466396\onestart-bin\chrome.VisualElementsManifest.xml **MD5:** 2E6DD0FB1979F75BDD8F9B8B0E069D9B **SHA256:** 9BADFCA9F104D331B03C9AECC02A1FD0FB25E0F3572A9B4D678BB747B88E342A	text
8648	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\SetupMetrics\2dbfe5c3-6d6d-4f78-83ae-a797c7cca59e.tmp **MD5:** 1B7CDDDFB06152AE01F12D9F253237D6 **SHA256:** FD668D6EDCF6B6CC176EDD9BF7B0D7F1881FE2F0D94EBAE656127C27A359550E	binary
2392	notification_helper.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\NotificationHelperMetrics\13831413-cffd-46e5-95ec-5daf7ed50d07.tmp **MD5:** C477B01F180588AEB403B320F1E6F731 **SHA256:** 4B9C56CE788E8A46E59195CAD48FA85A4360AF7F4407D4BD3EA63FB7D903B183	binary
2392	notification_helper.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat **MD5:** FC81892AC822DCBB09441D3B58B47125 **SHA256:** FB077C966296D02D50CCBF7F761D2A3311A206A784A7496F331C2B0D6AD205C8	binary
2392	notification_helper.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\NotificationHelperMetrics\20250307060845.pma **MD5:** C477B01F180588AEB403B320F1E6F731 **SHA256:** 4B9C56CE788E8A46E59195CAD48FA85A4360AF7F4407D4BD3EA63FB7D903B183	binary
8648	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\SetupMetrics\8648_13385801325700540.pma **MD5:** 1B7CDDDFB06152AE01F12D9F253237D6 **SHA256:** FD668D6EDCF6B6CC176EDD9BF7B0D7F1881FE2F0D94EBAE656127C27A359550E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\877e2293-feb7-4270-b6fa-fb1547771160.tmp **MD5:** CD375F88E8BE342D640B4E69DC5196A7 **SHA256:** 20657260B25D3A4ADE937F9BD57DA09260BA414183A48C27F5DEDAA7EB3152F9	binary
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\SetupMetrics\f9c0b152-7131-4c58-a1c3-be3ecea23e29.tmp **MD5:** 2DAFC52EA6E7AF28ED3922A67CD64035 **SHA256:** 1F7676B4364B74BD1A5E530595A4D86958B9D0BC51415B4E65FB29DB6ACF5174	binary
7740	setup.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\Application\SetupMetrics\7740_13385801325771894.pma **MD5:** 2DAFC52EA6E7AF28ED3922A67CD64035 **SHA256:** 1F7676B4364B74BD1A5E530595A4D86958B9D0BC51415B4E65FB29DB6ACF5174	binary
8852	msiexec.exe	C:\Windows\Temp\~DFA88EB60CD640DBB3.TMP **MD5:** C2849E3F8BB77902F631D90BD970D232 **SHA256:** FA4906B3C31BEE085DEC52C7FD39A237150BE53F73BAF6C94AF7BC384E693540	binary
8852	msiexec.exe	C:\Windows\Temp\~DF72B587B632C71A9C.TMP **MD5:** C2849E3F8BB77902F631D90BD970D232 **SHA256:** FA4906B3C31BEE085DEC52C7FD39A237150BE53F73BAF6C94AF7BC384E693540	binary
8852	msiexec.exe	C:\Windows\Installer\SourceHash{E26424D6-5AA5-419C-BBA9-6B1328F7A00B} **MD5:** 59D60808FB3EEC872E3F77DCF75C3527 **SHA256:** A2BBE917C9D0EC2522911130B034E4BC1BE405B3093CAAF32E4AD33DAB138112	binary
8852	msiexec.exe	C:\Windows\Temp\~DF1958EB8ABEC315AF.TMP **MD5:** BF619EAC0CDF3F68D496EA9344137E8B **SHA256:** 076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560	binary
8852	msiexec.exe	C:\Windows\Temp\~DFF91208219FA51645.TMP **MD5:** C7B0CCCC48A820E4DC6B0440D4E2ED09 **SHA256:** C7225399435F4E4C8BB5E58AC9BBD34EE7B83F3F0FA537697A96F2655B92133F	binary
8852	msiexec.exe	C:\Windows\Temp\~DF30F00D69E739BC01.TMP **MD5:** BF619EAC0CDF3F68D496EA9344137E8B **SHA256:** 076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560	binary
8852	msiexec.exe	C:\Windows\Temp\~DF402A3D74A0764D4E.TMP **MD5:** 95BF43BF9B2D03F1353B9B6ED319A995 **SHA256:** 2DF40272E3BE35022A30522F538ECCA445129CEC8EE8BBEB52BEA468E2EF9D5E	binary
8852	msiexec.exe	C:\Windows\Temp\~DF384AF16D4ACF040D.TMP **MD5:** BF619EAC0CDF3F68D496EA9344137E8B **SHA256:** 076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560	binary
8852	msiexec.exe	C:\Windows\Temp\~DF1099B53317CD72E9.TMP **MD5:** FE125FA3C2443A514ED7F090A5E36CE7 **SHA256:** 5CC6B4246C8EC29AEFE66F3466663EFD361CFABCCB8EAF8E9595CE33274B7088	binary
8852	msiexec.exe	C:\Windows\Temp\~DFA3DA31FBB7544822.TMP **MD5:** FE125FA3C2443A514ED7F090A5E36CE7 **SHA256:** 5CC6B4246C8EC29AEFE66F3466663EFD361CFABCCB8EAF8E9595CE33274B7088	binary
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSI1E57.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
8804	msiexec.exe	C:\Users\admin\AppData\Local\Temp\MSI1E27.tmp **MD5:** 0606E1A2FE0D72593405CAFEB945C740 **SHA256:** 7B3A4E3E3F58FA49164D49B14BC10C13A9D734846956C8A7A433C8BB6C82D983	executable
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\First Run	—

PID	Process	Filename	Type
		MD5: — SHA256: —	
8852	msiexec.exe	C:\Windows\Temp\~DFDADEC0D5490DFC41.TMP MD5: BF619EAC0CDF3F68D496EA9344137E8B SHA256: 076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Local State MD5: EDC6E54307B3351B83CE017EEC933D73 SHA256: 65736D4FFC49D438EDA891892D872229DDD94D0CD73003C36057229D046068D9	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Variations MD5: 961E3604F228B0D10541EBF921500C86 SHA256: F7B24F2EB3D5EB0550527490395D2F61C3D2FE74BB9CB345197DAD81B58B5FED	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Preferences MD5: 1258F94169747A03BF3ACFC60C2FDB77 SHA256: AB4A6D4F6BF33EDA1425907A6AE94B571411E6536C99D23AB53F52CDF7071A4E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\412b1f21-0123-4304-a836-7e64cb08f5eb.tmp MD5: EDC6E54307B3351B83CE017EEC933D73 SHA256: 65736D4FFC49D438EDA891892D872229DDD94D0CD73003C36057229D046068D9	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\ShaderCache\data_0 MD5: CF89D16BB9107C631DAABF0C0EE58EFB SHA256: D6A5FE39CD672781B256E0E3102F7022635F1D4BB7CFCC90A80FFFE4D0F3877E	vxd
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\ShaderCache\index MD5: 01E1B2C6DFB3117ADDB1AD703C16EFB7 SHA256: 9B5E0CA2561EBEE82373048F2C1AC8ADC374CC4F170E85815DD6AA52AAB53D5A	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\aa0102e4-333c-4c90-9c85-7d666204ef40.tmp MD5: F396CD780AF91BB2F7CA62825FBB03C7 SHA256: 93DF7202621390FF88D6B39347DEB4E3DA517C0CCECFF8B2F5F7ECEF61CA308F	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\ShaderCache\data_1 MD5: 259E7ED5FB3C6C90533B963DA5B2FC1B SHA256: 35BB2F189C643DCF52ECF037603D104035ECDC490BF059B7736E58EF7D821A09	vxd
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\ShaderCache\data_2 MD5: 0962291D6D367570BEE5454721C17E11 SHA256: EC1702806F4CC7C42A82FC2B38E89835FDE7C64BB32060E0823C9077CA92EFB7	vxd
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\InterestGroups-journal MD5: CFB8FA8A8FDAC240A0E13F3EFCAE7BD7 SHA256: 7DBED02F50CE2219B6798B72A6520B0309C4D64B8942F2AD92DDA216B7F2ACE5	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\index-dir\temp-index MD5: B5CAE43ED00F18C8B1C38405B24D7105 SHA256: E8C46BE1CAF8D4DBC9CD112F4A0B9B147CC66C37671E8F8CEE98EA16F984CCC2	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\wasm\index MD5: 54CB446F628B2EA4A5BCE5769910512E SHA256: FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\wasm\index-dir\temp-index MD5: 19EE769FDD20E61F1E79E01695C6DA5B SHA256: F4C81029A17FFB7E5E8860A4AB5ADF79BF81FA789E077D618911A204162EF82E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\index MD5: 54CB446F628B2EA4A5BCE5769910512E SHA256: FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\wasm\index-dir\the-real-index MD5: 19EE769FDD20E61F1E79E01695C6DA5B SHA256: F4C81029A17FFB7E5E8860A4AB5ADF79BF81FA789E077D618911A204162EF82E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\SharedStorage-journal MD5: A6F8403BE78EA3A74C2ED819019EC8F4 SHA256: 4C2E44AE89DB81CD15F825081641FCD5A91B70A83B66208DFA87E1683ABD8021	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Last Version MD5: 7519C5D1B5AD7B70A27700B27CBF546F SHA256: D0918E4DA8CC23D672882693F40BDC167B1664339B15BFC1A35F5FE04D7FB8A4	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Site Characteristics Database\000001.dbtmp MD5: 46295CAC801E5D4857D09837238A6394 SHA256: 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sync Data\LevelDB\000001.dbtmp MD5: 46295CAC801E5D4857D09837238A6394 SHA256: 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sync Data\LevelDB\CURRENT MD5: 46295CAC801E5D4857D09837238A6394 SHA256: 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\History-journal MD5: — SHA256: —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\index-dir\the-real-index MD5: B5CAE43ED00F18C8B1C38405B24D7105 SHA256: E8C46BE1CAF8D4DBC9CD112F4A0B9B147CC66C37671E8F8CEE98EA16F984CCC2	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Local State~RF122f26.TMP MD5: EDC6E54307B3351B83CE017EEC933D73 SHA256: 65736D4FFC49D438EDA891892D872229DDD94D0CD73003C36057229D046068D9	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sync Data\LevelDB\MANIFEST-000001 MD5: 5AF87DFD673BA2115E2FCF5CFDB727AB SHA256: F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\ShaderCache\data_3 MD5: 41876349CB12D6DB992F1309F22DF3F0 SHA256: E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C	vxd
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\a0e73d63-78a4-44c4-91af-81e243c0e3a7.tmp	binary

PID	Process	Filename	Type
		MD5: 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\History **MD5:** 9B85A4B842B758BE395BC19ABA64799C **SHA256:** ECC8D7540D26E3C2C43589C761E94638FC5096AF874D7DF216E833B9599C673A	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Rules\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Google Profile.ico **MD5:** 70E5D4E286C45331931C22DBF5B15A9B **SHA256:** 6FD93AA2E71AE66DF17C2E84E719D27DF69762375894522D80C95D7C82393793	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Rules\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Rules\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Site Characteristics Database\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Scripts\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Site Characteristics Database\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Affiliation Database **MD5:** C94F7E7ABFC9942BAE7098B53DEF6FEE **SHA256:** 20FB68D08674A2FA9FCB64A6CC6B299EF0112429EA96BEE5D48D883C0A7AEC2F	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\metadata\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Scripts\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Google Profile.ico~RF1231f5.TMP **MD5:** 70E5D4E286C45331931C22DBF5B15A9B **SHA256:** 6FD93AA2E71AE66DF17C2E84E719D27DF69762375894522D80C95D7C82393793	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\7dda6dba-9af2-4daa-b74b-720a20ae4d40.tmp **MD5:** 70E5D4E286C45331931C22DBF5B15A9B **SHA256:** 6FD93AA2E71AE66DF17C2E84E719D27DF69762375894522D80C95D7C82393793	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension State\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\metadata\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\metadata\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Scripts\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3192	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Storage\leveldb\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\cc1d141c-30dc-4802-9220-c8fab5f7326a.tmp **MD5:** 70E5D4E286C45331931C22DBF5B15A9B **SHA256:** 6FD93AA2E71AE66DF17C2E84E719D27DF69762375894522D80C95D7C82393793	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension State\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Google Profile.ico~RF123224.TMP **MD5:** 70E5D4E286C45331931C22DBF5B15A9B **SHA256:** 6FD93AA2E71AE66DF17C2E84E719D27DF69762375894522D80C95D7C82393793	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Storage\leveldb\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3192	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Storage\leveldb\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension State\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
3192	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Session Storage\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\bed96ec9-68ef-4f42-bd06-58fd901dad2e.tmp	image

PID	Process	Filename	Type
		MD5: 70E5D4E286C45331931C22DBF5B15A9B **SHA256:** 6FD93AA2E71AE66DF17C2E84E719D27DF69762375894522D80C95D7C82393793	
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
3192	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Session Storage\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\5e059565-837c-44ec-802e-804813d4cc80.tmp **MD5:** 70E5D4E286C45331931C22DBF5B15A9B **SHA256:** 6FD93AA2E71AE66DF17C2E84E719D27DF69762375894522D80C95D7C82393793	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GPUCache\index **MD5:** B7D2B7550F5EC40302BDEF51C62562F6 **SHA256:** 74D6BD791A0F5A93AD78FB589A826498B061FF6C50B5B4D89F389FE1A1F608D2	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Google Profile.ico~RF123262.TMP **MD5:** 70E5D4E286C45331931C22DBF5B15A9B **SHA256:** 6FD93AA2E71AE66DF17C2E84E719D27DF69762375894522D80C95D7C82393793	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Session Storage\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GPUCache\data_0 **MD5:** CF89D16BB9107C631DAABF0C0EE58EFB **SHA256:** D6A5FE39CD672781B256E0E3102F7022635F1D4BB7CFCC90A80FFFE4D0F3877E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GPUCache\data_1 **MD5:** 259E7ED5FB3C6C90533B963DA5B2FC1B **SHA256:** 35BB2F189C643DCF52ECF037603D104035ECDC490BF059B7736E58EF7D821A09	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GPUCache\data_2 **MD5:** 0962291D6D367570BEE5454721C17E11 **SHA256:** EC1702806F4CC7C42A82FC2B38E89835FDE7C64BB32060E0823C9077CA92EFB7	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Shared Dictionary\cache\index **MD5:** 54CB446F628B2EA4A5BCE5769910512E **SHA256:** FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Shared Dictionary\cache\index-dir\temp-index **MD5:** 039ACA3D8528CA29BD5D78D2B23F0953 **SHA256:** 4A321235ACFFA63330737F59E0896E386A48075DDF773BCF3CD4571B09C9DFF0	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Shared Dictionary\cache\index-dir\the-real-index **MD5:** 039ACA3D8528CA29BD5D78D2B23F0953 **SHA256:** 4A321235ACFFA63330737F59E0896E386A48075DDF773BCF3CD4571B09C9DFF0	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GPUCache\data_3 **MD5:** 41876349CB12D6DB992F1309F22DF3F0 **SHA256:** E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnWebGPUCache\index **MD5:** DF1B3723271A80335B23E6DB80333F40 **SHA256:** 826CA084502817180E5520218DFD984F76593C43806A3E6A33D57FEAB1C85C43	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\654a892a-010a-4cee-b5c2-f776dbc9b88e.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\SCT Auditing Pending Reports **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnWebGPUCache\data_0 **MD5:** CF89D16BB9107C631DAABF0C0EE58EFB **SHA256:** D6A5FE39CD672781B256E0E3102F7022635F1D4BB7CFCC90A80FFFE4D0F3877E	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\Trust Tokens **MD5:** D25D5E1DC1D93430E64EE17E48CE442E **SHA256:** 8C471CAB38A1696289186D01B06FF6AF2A888852DC18D6FB8D2A0E54898104ED	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnWebGPUCache\data_1 **MD5:** 259E7ED5FB3C6C90533B963DA5B2FC1B **SHA256:** 35BB2F189C643DCF52ECF037603D104035ECDC490BF059B7736E58EF7D821A09	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\ad64bbdd-b25d-4cda-b3f9-05fce3ab7cd6.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnWebGPUCache\data_2 **MD5:** 0962291D6D367570BEE5454721C17E11 **SHA256:** EC1702806F4CC7C42A82FC2B38E89835FDE7C64BB32060E0823C9077CA92EFB7	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnGraphiteCache\data_1 **MD5:** 259E7ED5FB3C6C90533B963DA5B2FC1B **SHA256:** 35BB2F189C643DCF52ECF037603D104035ECDC490BF059B7736E58EF7D821A09	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnWebGPUCache\data_3 **MD5:** 41876349CB12D6DB992F1309F22DF3F0 **SHA256:** E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnGraphiteCache\data_0 **MD5:** CF89D16BB9107C631DAABF0C0EE58EFB **SHA256:** D6A5FE39CD672781B256E0E3102F7022635F1D4BB7CFCC90A80FFFE4D0F3877E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnGraphiteCache\data_2 **MD5:** 0962291D6D367570BEE5454721C17E11 **SHA256:** EC1702806F4CC7C42A82FC2B38E89835FDE7C64BB32060E0823C9077CA92EFB7	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnGraphiteCache\index	binary

PID	Process	Filename	Type
		MD5: 172491AEDDC36011A847CE4E477FDC64 **SHA256:** C9CCE4F2EC90058E313207414912D2C435F2B6297898C8DE1D9607621CA512F6	
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\SCT Auditing Pending Reports~RF12338b.TMP **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GrShaderCache\index **MD5:** C5EECBE0AE84516AB91F22A72FCCD36B **SHA256:** 04D376F552D42A39714CCBD8DA7D59EB838D1FE00A866089DC6D0511B1B79308	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DawnGraphiteCache\data_3 **MD5:** 41876349CB12D6DB992F1309F22DF3F0 **SHA256:** E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GrShaderCache\data_1 **MD5:** 259E7ED5FB3C6C90533B963DA5B2FC1B **SHA256:** 35BB2F189C643DCF52ECF037603D104035ECDC490BF059B7736E58EF7D821A09	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GraphiteDawnCache\index **MD5:** 1956BD07A935994373BDD56378F7C287 **SHA256:** —	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GrShaderCache\data_0 **MD5:** CF89D16BB9107C631DAABF0C0EE58EFB **SHA256:** D6A5FE39CD672781B256E0E3102F7022635F1D4BB7CFCC90A80FFFE4D0F3877E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GrShaderCache\data_3 **MD5:** 41876349CB12D6DB992F1309F22DF3F0 **SHA256:** E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GrShaderCache\data_2 **MD5:** 0962291D6D367570BEE5454721C17E11 **SHA256:** EC1702806F4CC7C42A82FC2B38E89835FDE7C64BB32060E0823C9077CA92EFB7	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GraphiteDawnCache\data_1 **MD5:** 259E7ED5FB3C6C90533B963DA5B2FC1B **SHA256:** 35BB2F189C643DCF52ECF037603D104035ECDC490BF059B7736E58EF7D821A09	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\index **MD5:** 3E61C8469EB2DFC00C1909A1E99562CC **SHA256:** 6D596FBAE72A65DBD91BB1C11ED006C2C697AC94E2D585FADE991CDCC9A9A368	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GraphiteDawnCache\data_0 **MD5:** CF89D16BB9107C631DAABF0C0EE58EFB **SHA256:** D6A5FE39CD672781B256E0E3102F7022635F1D4BB7CFCC90A80FFFE4D0F3877E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GraphiteDawnCache\data_2 **MD5:** 0962291D6D367570BEE5454721C17E11 **SHA256:** EC1702806F4CC7C42A82FC2B38E89835FDE7C64BB32060E0823C9077CA92EFB7	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\GraphiteDawnCache\data_3 **MD5:** 41876349CB12D6DB992F1309F22DF3F0 **SHA256:** E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\data_0 **MD5:** CF89D16BB9107C631DAABF0C0EE58EFB **SHA256:** D6A5FE39CD672781B256E0E3102F7022635F1D4BB7CFCC90A80FFFE4D0F3877E	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\data_1 **MD5:** 259E7ED5FB3C6C90533B963DA5B2FC1B **SHA256:** 35BB2F189C643DCF52ECF037603D104035ECDC490BF059B7736E58EF7D821A09	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\data_2 **MD5:** 0962291D6D367570BEE5454721C17E11 **SHA256:** EC1702806F4CC7C42A82FC2B38E89835FDE7C64BB32060E0823C9077CA92EFB7	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\data_3 **MD5:** 41876349CB12D6DB992F1309F22DF3F0 **SHA256:** E09F42C398D688DCE168570291F1F92D079987DEDA3099A34ADB9E8C0522B30C	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\trusted_vault.pb **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_000001 **MD5:** 0BA0131F533E1E02995E23F0E5BC3072 **SHA256:** —	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\1f094705-0fa1-4248-ae66-eec22628478b.tmp **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_000002 **MD5:** 2749599D0C760696078E0DD60CEAFB68 **SHA256:** B55B06AA049446C48B48F4C36C0588B290E292A12EAA394E6F4E9B95F6689152	compressed
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\23fb9215-cc85-4de6-8698-f20a398ba158.tmp **MD5:** AF8E621AC13ACB0A44D63EDCE4DBAFAA **SHA256:** C0289FDCD971B0DFBA34BA844F9A99B6C13780C527171823B2CD4926BCBE0490	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\915ec6bb-9422-4713-8161-8f7d136eb15f.tmp **MD5:** 6E9E9F9B768F18D0E82237867B24A457 **SHA256:** E98A028782F27E3D33C14D00287D998A26DBDB81965D852577639A8729A431A8	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\e7dbc6ed-86b0-4249-87a5-67da5821fdb7.tmp **MD5:** 22F34F3C8E6CACD4D7C97C65F67C82B6 **SHA256:** 85DA821899515CE243833A2E057C80FD43E545EAABF31C68B871D6AD19E14D93	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF123d7e.TMP **MD5:** FE86F804921307EA5BE22FC8424AE066 **SHA256:** 9361639248DD652E2B6489DFFA4E053ED63419D66DD78A3614F9641ABD2F3FB5	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_000004 **MD5:** 0DC52D5156E0E3423A20671F85112A3A **SHA256:** 55D8D47F45278ED4E61568932ABC7DBBF8111BFD5F815A5FF0B90120C238551F	compressed
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\246acda8-80dc-4e31-be7f-64a909fa8a5c.tmp	binary

PID	Process	Filename	Type
		MD5: 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_000003 **MD5:** 9ECD937E59F04291B27F9A13BCECEBEA **SHA256:** 3093793A6F48BBDB0346098AEAE29056719507430374F26DE550BB1D033E5CE7	compressed
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DIPS **MD5:** DE6318A2E388B7D7A50755D882AA0185 **SHA256:** 1532DF821F0835D2E6B5AE7368ACDC66C9D1F468A0C0D029B69AEE5AD74C9C75	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_1986788537\23fb9215-cc85-4de6-8698-f20a398ba158.tmp **MD5:** AF8E621AC13ACB0A44D63EDCE4DBAFAA **SHA256:** C0289FDCD971B0DFBA34BA844F9A99B6C13780C527171823B2CD4926BCBE0490	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network Action Predictor **MD5:** D25D5E1DC1D93430E64EE17E48CE442E **SHA256:** 8C471CAB38A1696289186D01B06FF6AF2A888852DC18D6FB8D2A0E54898104ED	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\0ffaddaa-3372-4954-8c2e-04a1808db5f1.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\f0d49fac-4d5a-4657-a06e-fab6be3ee9b8.tmp **MD5:** EBBC644608F04D59A0CF4574FD82A205 **SHA256:** 05A050E11E24620F4632F237E253247B92B3B78C85CA162B9315B2DCFC457308	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Last Browser **MD5:** 311CBAC7B1C2B139C9E1D75D0EADE725 **SHA256:** 389A994E43D584B4B1E2DB612830D057FE9296FCDF0F7C4FE58A38A0D67BEA7A	binary
7596	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_1986788537\CRX_INSTALL\manifest.json **MD5:** 245E3B5D1A0B49FC98299B9D8050AA60 **SHA256:** FC560442B53C3DFF65D9F2A9D5007E335C6A1E79407851F669C2D64EB016C6A3	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\915ec6bb-9422-4713-8161-8f7d136eb15f.tmp **MD5:** 6E9E9F9B768F18D0E82237867B24A457 **SHA256:** E98A028782F27E3D33C14D00287D998A26DBDB81965D852577639A8729A431A8	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Bookmarks **MD5:** EBBC644608F04D59A0CF4574FD82A205 **SHA256:** 05A050E11E24620F4632F237E253247B92B3B78C85CA162B9315B2DCFC457308	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GCM Store\Encryption\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\BrowsingTopicsSiteData **MD5:** C2680B82D7A08A6421FA01F1BEAE4EAA **SHA256:** 06AB381E06178F2A0062DB9B1D069ADF065C4FF00232426B8D70FA3AD7703A76	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\PreferredApps **MD5:** 2B432FEF211C69C745ACA86DE4F8E4AB **SHA256:** 42B55D126D1E640B1ED7A6BDCB9A46C81DF461FA7E131F4F8C7108C2C61C14DE	binary
8632	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\CRX_INSTALL\manifest.json **MD5:** BA33BC2D4EEAB04371667A60CDCE6FF4 **SHA256:** B31B3B0658E0AB67F9BE91D22988B92E956F48D1C87048AA9CA9652440F52800	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GCM Store\Encryption\000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GCM Store\Encryption\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
4300	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\CRX_INSTALL\page.js **MD5:** 44C3536B164EB520ECFD6744DE59CD67 **SHA256:** 0D62909009698FAC935C0CDFC895A0A3E069E176B59B386D85C31C6C9A30EC2A	binary
4300	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\CRX_INSTALL\serviceWorker.js **MD5:** 2CB81A569B3D4FBB825401B41FBF1F3E **SHA256:** 95E631F1C1078F6FF1BE4BD9A3303265AAB74E8D418EC03D21D1E71B0CC906CF	binary
4300	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\CRX_INSTALL\images\icon-128.png **MD5:** FC353010CCB8DB812FC087D91B1F8FF5 **SHA256:** 270A86C434BA18125FBF1803B9096EBBEC57DA6F732AAB32D0412EB72B940365	image
4300	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\CRX_INSTALL\images\icon-48.png **MD5:** 86767A88F1F762D1D1FB9D2D9FCE7E25 **SHA256:** C3BB95C5613F101335DADF1193CDA8B7D9C2FA7C114F01B8F51F54196E51E354	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\ScriptCache\index **MD5:** 54CB446F628B2EA4A5BCE5769910512E **SHA256:** FBCFE23A2ECB82B7100C50811691DDE0A33AA3DA8D176BE9882A9DB485DC0F2D	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\CRX_INSTALL\images\icon-128.png **MD5:** CC2E0134420F798CCC1119101273C7DC **SHA256:** 04EA165A577CA239E95085C6A0011E06A76D4E3DA4D8BDADDD624B5ADAD23753	image
8912	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_1986788537\CRX_INSTALL\bg.js **MD5:** 6ADC10DD97401B10229F53676CEC152D **SHA256:** 63B521B6ECBCE6826F89021048EEEDC46E1B00C3A80B81DA5C5819CF82C5F352	text
4300	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\CRX_INSTALL\images\icon-16.png **MD5:** BDF3ED93CBCF791497F49EFA2333BC2C **SHA256:** C0CD4F4F174140CE35CA746A225A77571D332A49C0D15B1F2E0CB1142FDA3B2F	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\Database\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\Database\CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\Database\000001.dbtmp	text

PID	Process	Filename	Type
		MD5: 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\ScriptCache\index-dir\temp-index **MD5:** 7099556B67CEE084B3803E96967596B0 **SHA256:** CA6692459CB314DC4D8F2E339B788DAD0B2BC58B21E3E574D9238FFC5878A970	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\CRX_INSTALL\images\icon-16.png **MD5:** DAD5CF43DCEFC9C2DF59A3AE65C789B7 **SHA256:** 2CF5994006C84B95B72772116D17B2592FB1760BD9F9359D58C8F3C875C1F567	image
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_993984723\CRX_INSTALL\images\icon-48.png **MD5:** E975EFF68B460850BDF7EDF84D5C75DC **SHA256:** A7FEE3D6FDF1958859B546D99447A6A7F9E54263AB0A39DBB72070B3573671F3	image
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\chrome_url_fetcher_1280_1790636402 \oimompecagnajdejgnnjijobebaeigek_4.10.2891.0_win64_acwxtxt2znguar3w2o252umtomsq.crx3 **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\component_crx_cache \oimompecagnajdejgnnjijobebaeigek_1.a6af95a209b2e652ed6766804b9b8ad6b6a68f2c610b8f14713cd40df0d62bf9 **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index **MD5:** 7099556B67CEE084B3803E96967596B0 **SHA256:** CA6692459CB314DC4D8F2E339B788DAD0B2BC58B21E3E574D9238FFC5878A970	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\ScriptCache\2cc80dabc69f58b6_0 **MD5:** 8D1156EB71BA8CC8340339A34F4A96C6 **SHA256:** D1023688E2441D43E8A2CBF41A9C20A57B04ECE5EA214AE476992B4D585FCB12	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\ScriptCache\2cc80dabc69f58b6_1 **MD5:** 6E0A16036CA31D2A7C9E4D11DDB1B331 **SHA256:** 415C24331F12491481EC1D79FFA0971A7C2326916C203724E750B6AE9F6D60CC	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Extension Settings\memhbiihnoblfombkckdfmemihcnlihc \CURRENT **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Extension Settings\memhbiihnoblfombkckdfmemihcnlihc \000001.dbtmp **MD5:** 46295CAC801E5D4857D09837238A6394 **SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443	text
8668	onestart.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1280_1509415995_metadata\verified_contents.json **MD5:** E88D7CBB64F8AD6EB60E61C46A67840E **SHA256:** 9B791C9F3350A7B4EF88F1837FCD7A1DF7C51E0D0AF13DFFED00B5E9817C4CDA	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\e2252aa6-a329-4701-9438-a9440bdf4709.tmp **MD5:** 26149E076CFBD70FEBF9750B95205F2A **SHA256:** 7C5100042DE177EFA426459FC652A2D454A4EC1794DA08352765A97F05F922B0	binary
8668	onestart.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1280_1509415995_platform_specific\win_x64\widevinecdm.dll.sig **MD5:** BF85030725211B1D56494B40FB88C6F9 **SHA256:** BDAE7B6C2DE3587282809F2EE1B07DB0B29769DE2CE9AEC06F4399685C7729B7	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\BrowsingTopicsState **MD5:** 26149E076CFBD70FEBF9750B95205F2A **SHA256:** 7C5100042DE177EFA426459FC652A2D454A4EC1794DA08352765A97F05F922B0	binary
8668	onestart.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1280_1509415995\LICENSE **MD5:** F6719687BED7403612EAED0B191EB4A9 **SHA256:** AFB514E4269594234B32C873BA2CD3CC8892E836861137B531A40A1232820C59	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\25297ff9-88b4-4c8b-acd3-e6ce65d4e913.tmp **MD5:** 305B26BB6CEFA1239179C5ACC67313AE **SHA256:** B9065C41F64E73F21C0E120488654E5A63918B9A3FF95DA3A9C1705C9B74485E	binary
8668	onestart.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1280_1509415995_platform_specific\win_x64\widevinecdm.dll **MD5:** 1B32D1EC35A7EAD1671EFC0782B7EDF0 **SHA256:** 3ED0DEC36754402707C2AE4FBFA887FE3089945F6F7C1A8A3E6C1E64AD1C2648	executable
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-af.hyb **MD5:** FFA9DB945F0F0C15B8BBA75A6E064880 **SHA256:** 5487EE44A4CD706D0086522E90C59C76CDF2AC68CE506FD3EAE6054B9220C0CF	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-be.hyb **MD5:** 087DE134F3B23A9944AFD711A9667A0B **SHA256:** 25B7CFA039F82AC92990E1789DE40988D490DB9B613852FB24036B38FF87893C	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-as.hyb **MD5:** 8961FDD3DB036DD43002659A4E4A7365 **SHA256:** C2784E33158A807135850F7125A7EAABE472B3CFC7AFB82C74F02DA69EA250FE	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1280_1509415995\manifest.fingerprint **MD5:** D9013E7945FBBB5AFD78207422B28768 **SHA256:** 91F515E8B56C8234D78C1436BD38E7353DBA33EBF53CA0EB0CE599A23F3A4360	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Local State~RF125607.TMP **MD5:** F396CD780AF91BB2F7CA62825FBB03C7 **SHA256:** 93DF7202621390FF88D6B39347DEB4E3DA517C0CCECFF8B2F5F7ECEF61CA308F	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\7c8a325c-4954-4b15-9a91-baaae7521af3.tmp **MD5:** B3C8885668920A7A37C0CB4E8B59FC78 **SHA256:** F691DC79E3F5DA221D8373A84759CE715C6E599F446C0452F3908E48E7957035	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-bg.hyb **MD5:** E8A4F8F5238F9A0FF6968AD8DBA2755F **SHA256:** 7593F0395081E3EEB2D8516D10746608AFD826CFFD4E7E37D53936993D200A13	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-bn.hyb **MD5:** 8961FDD3DB036DD43002659A4E4A7365 **SHA256:** C2784E33158A807135850F7125A7EAABE472B3CFC7AFB82C74F02DA69EA250FE	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-cy.hyb	binary

PID	Process	Filename	Type
		MD5: B0F32ED7B4B8A068A962D820627B7229 **SHA256:** 4D0569FE2F4B41B3164CF610310E1D996FD2C553CC39DE6062E50F4E033CC207	
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-cs.hyb **MD5:** E8B1509F86508E807D61216614B3DD58 **SHA256:** 97A4755FE9E653A08969F1933E3DB19C712078B227BD5AA6799093ABC5A0EDC3	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-da.hyb **MD5:** D0E160DCA547EDA390D6CC7C4A1F7AC6 **SHA256:** 86FDFC8DB62CDAA11F615DAD3712DA1F4708294E029A4AAD0FC285D4EA16C4BD	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-de-1901.hyb **MD5:** DD9D0A81D897F88F76C1F6D69FB7483E **SHA256:** 8C5FA4B29519D17593E923BC6A9A284DF7A6D07FAC42F897110B8FB2E0BAEEF5	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-cu.hyb **MD5:** B4E5921B1DF85BA9F2EBE6CE578915F6 **SHA256:** 2BAEE19D5024FF87DCF3A1B9D0DA1B3AC5A1E506ADEEAD3B96A4DE5395D0290E	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-de-1996.hyb **MD5:** E7A9906B316D478B55BF8EBCBBB1D1C5 **SHA256:** D673805547A0228D2F57A5AD551B8760CFCC521F38C49284ED3976E3515BCA49	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-el.hyb **MD5:** 746A59E9F9DDA15C0F17C1B72921C85F **SHA256:** 76AE3454FB0045ADB83094832578AA4749CE4DC694C4EDCF85B419C1E2D9BCD3	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-en-gb.hyb **MD5:** FA3DCB77293A058277CB148A0FF491FA **SHA256:** AE4B78009D18E849D87458677151EE3AAD1608AD72EC050DFD2421D22E7D031F	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-eu.hyb **MD5:** E90EA97070CFCFA795FBD807AC300D34 **SHA256:** E2778A4FC7B8F064A32B6A44BC29F10E264D9D6214B8EDB8EBD1F5F6D68E2EB2	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-es.hyb **MD5:** F6BD0377237FCA3C4B7C6A6CB244298B **SHA256:** 137461792537A2E56A6475E81E2B9AD7A2BDABF1F4738FAE186DCA3022357349	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-gl.hyb **MD5:** 1B08FB098D29C30488B8FC3F19DCF8B9 **SHA256:** 89D98EFF14E2CF1C2314EFDF392339E62D7E786F100202A7377BF7B22095A0C5	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-de-ch-1901.hyb **MD5:** C6773229845710633D3A4D6DD9800FC5 **SHA256:** 8223A912160354E05735522FDB339DC59B353AD5D1E4F4CFA94898DC348E748F	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-ga.hyb **MD5:** 768032A419E0AE3BD870D591E2173715 **SHA256:** 1E3043F395BFB2A4C43D0480BA2F168ED622881CC3482359CA6E99821E983BE8	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-fr.hyb **MD5:** 092E0A95D6DADA26CA56D2ED558749A3 **SHA256:** 00BD8B2D398D77575DA2BFBBC5EC641AAD7F2A87D4A31186EC169E85A27DE5B7	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-et.hyb **MD5:** 2AE42AB807286F6EC0FF1876D9536B0B **SHA256:** 10079C66014DD2E6ABFEF5A018E6553FD5A036AFB96BD2A235440A188F88B15E	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-en-us.hyb **MD5:** B2693233D14890C81D322BEC948549E7 **SHA256:** 03727CD6F4AA71B203C4C74CA6987AC7D87F13037337AC6F4B6996C2A0DC5F8C	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-gu.hyb **MD5:** F6DC4E0FB974869D3D9457C582A38690 **SHA256:** AF0EDB67C2219B803C3EB6C1DEE6F2D41A3FE00468A9DA8BE8EF5056D701ABF3	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-hi.hyb **MD5:** 0807CF29FC4C5D7D87C1689EB2E0BAAA **SHA256:** F4DF224D459FD111698DD5A13613C5BBF0ED11F04278D60230D028010EAC0C42	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-hy.hyb **MD5:** 70EA4451C3A26FD7197A3D2188BE4152 **SHA256:** 9B34DFCA85CB27546829F104F137757EFB274934C1E9D4991F55AD564962A76A	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-hr.hyb **MD5:** 1864E47E724BB7F9C052A2840EEE21D9 **SHA256:** D5F066A5657F1D7C39D053956DF204B7926F40D2FE4F69573AF09D909066E26C	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-hu.hyb **MD5:** 37B1F197E8DFBAFDAC4597EDCF673E63 **SHA256:** 8B3A16268CC932B226C17FF405B3CFB6EB38A9511A2043D653DC03729EFCEAC1	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-it.hyb **MD5:** A4D5EC24D4C5EE745CDCDC019018074F **SHA256:** F9C027D7FD44B01CD5E1CDF802E20C63560673098AF18BEA0930BA9AF334E0F7	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-kn.hyb **MD5:** D986AC2E7C75CF3EF929A7A269AE0D5A **SHA256:** 2B999D0A152F804601AA8F38FF0D3A6E5949977BF1DAA76FA888ACAE21526287	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-ka.hyb **MD5:** AA6C771083158380B2631F01E3F64F20 **SHA256:** 2472271C7955C67E9FDB86D0CD3C5D88F5E598DA4F44B6741284B2BBCB2E4D52	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-nl.hyb **MD5:** D3BB05944DE3D0D7186E7E9383805E2C **SHA256:** 5EBDE398944B461CF940F0520C5A49C0882B6F36F9AC5CDA0538C8C8B44FB7CA	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-la.hyb **MD5:** 9AAA47272099A013A4389BC314B7D2ED **SHA256:** FD4B6F36135CD3B932E350EC2017DFD89D2E36AC226F54E4C8F2E4BC6DB0593D	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-mul-ethi.hyb **MD5:** B42317960E5DA868A8120CB79A440ABF **SHA256:** F2FAC1BD069FFE5CD1112D94CC31137ED38A1B161093ECD74C9C1688428B688B	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-mr.hyb	binary

PID	Process	Filename	Type
		MD5: 0807CF29FC4C5D7D87C1689EB2E0BAAA **SHA256:** F4DF224D459FD111698DD5A13613C5BBF0ED11F04278D60230D028010EAC0C42	
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-mn-cyrl.hyb **MD5:** 07CDA8332B62726883B29290CA35FC89 **SHA256:** 0D2731F16AA2C90FAEC8E63260358CBCCEDE403FAF95E3AF8C66BC2DB0729CA0	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-ml.hyb **MD5:** 84A0A36EA2C5B3209A3CD40D1043230F **SHA256:** 90572DB8F49B01EC6A102732CDF14FC3F07D363CBE0D261103E583043164E888	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-lv.hyb **MD5:** 05DFDB7F1EE5744573CCD62AE565B2C7 **SHA256:** 65962CCB5055E4C693E5AC493D6AFFDC810EC168EB2942F5705B7F4E464F9993	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-nb.hyb **MD5:** 677EDD1A17D50F0BD11783F58725D0E7 **SHA256:** C2771FBB1BFFF7DB5E267DC7A4505A9675C6B98CFE7A8F7AE5686D7A5A2B3DD0	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-lt.hyb **MD5:** 970C2671EAC4FFF6D840DC122E43B7C6 **SHA256:** 6FE2DA26A96834FB9AECBE586D40F728DF0EF676A4F235450054E66841B9E2CA	binary
8668	onestart.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1280_1509415995\manifest.json **MD5:** 32AEACEDCE82BAFBCBA8D1ADE9E88D5A **SHA256:** 4ED3C6389F6F7CD94DB5CD0F870C34A296FC0DE3B1E707FCCF01645B455790CE	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-nn.hyb **MD5:** F2D8FE158D5361FC1D4B794A7255835A **SHA256:** 5BCBB58EAF65F13F6D039244D942F37C127344E3A0A2E6C32D08236945132809	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-or.hyb **MD5:** 7E265A294303F69AA66C243F5F474463 **SHA256:** 4E9CD302BAFFC4EA3E9652327EA24072EBF37B5C4FC0719292BDAC10AAAD665B	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-pt.hyb **MD5:** 564FF32DED64C6BFC693F2758A53D68E **SHA256:** F6FBF1BCB260CC86256FC494F388F7B27D10865FBF8F61517DEE25AF4D58D6E8	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-pa.hyb **MD5:** 0F27E5BCCC1CD9DDF3EAC020DA27DA57 **SHA256:** 470329D28FAA484F945D78FFEFB176DCB6F2032C753E25BC014106AD24B2C68A	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-sk.hyb **MD5:** CEA295E8B4B99F95738727905A9184E2 **SHA256:** 138C5990961DA21993653F54A413DDACB8921D6D70B892B7CA154D6E8AD2028C	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-ru.hyb **MD5:** 4D132AB42E0C8ABD3BA93D8B34BDBEB3 **SHA256:** 336CE2048FFD31B7BCAF435E53BADFAF0579E405042D49ADBC0823F6BE5F9614	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-sl.hyb **MD5:** A21358DD4506643486F72F7D80D60A5B **SHA256:** AD746C68562603AC3B15E89DA03C76E081C08E7D9C8D4C9F64763E53D696C77C	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-ta.hyb **MD5:** AB2F6F9696FC7D699356244725E7C778 **SHA256:** 40FDA94856A86F065DE8BAA6184EA63DCDB011EE4CA498A7C1FEE44C99314C67	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-sq.hyb **MD5:** A22D0F39CD83F3A8E251F95C5B12DD31 **SHA256:** BC29C9401CE952414CBAEBC5C8EE1D27C1706C6F77807B5FF713E2124438B3CA	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-sv.hyb **MD5:** 892598DC59CE71E68ED337ED9FF3ABC1 **SHA256:** 56642AA5A37625FF9D034761D16B034D4BA5BE74090CBD825956BBCE2775ECD1	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-tk.hyb **MD5:** ED60185B6F455B6F8ED27EAEB73334A9 **SHA256:** 77FDAED29BD842AAA976AB7EF81B617A15C0A2D1EBD1161C1BF26B79A108B5CD	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\manifest.json **MD5:** 2617C38BED67A4190FC499142B6F2867 **SHA256:** D571EF33B0E707571F10BB37B99A607D6F43AFE33F53D15B4395B16EF3FDA665	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-te.hyb **MD5:** BF9DF63B3C97DE3BFF99E24EE4BC5F2E **SHA256:** 516FA9654FA3AEAAB480D40EAF6AD78FC039086BD8EDC144BE3D59525EDCAC29	binary
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-und-ethi.hyb **MD5:** 4AA9B2C0C9CCDE5140D01DC6502242BB **SHA256:** 1DE83CB787DFAF53FB7E6E8DB3AAE5008AD24EBDD28BE02031306EA9E9F3E285	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Top Sites-journal **MD5:** — **SHA256:** —	—
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\hyph-uk.hyb **MD5:** 0EC028755F0CD9EBBA41FB7273DE8BAF **SHA256:** 1C626ABE40D43F6D56A01B5B40305D7C7D6481F616EAC00A3F3AAAACA8388786	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF12481d.TMP **MD5:** CD375F88E8BE342D640B4E69DC5196A7 **SHA256:** 20657260B25D3A4ADE937F9BD57DA09260BA414183A48C27F5DEDAA7EB3152F9	har
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\6723f31e-da47-4c01-b02f-27742fbd5b7e.tmp **MD5:** 9E87939D19461A83683F525B3CF959B8 **SHA256:** 8BABC981574586EBD959E9B2CDDB3764B5D94AE90CE0788FF1A2BDB431233E13	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\4e8815b1-099c-4693-bc9d-ebfddbb1c689.tmp **MD5:** 2FEFB23BCA5580606BA16A2DB319093C **SHA256:** 8F1DC9DEAFA8E374E371E19F97B7C4FDEDB5FAF91C16CA0DF242E6C2A1114A2C	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Preferences~RF125859.TMP **MD5:** 1258F94169747A03BF3ACFC60C2FDB77 **SHA256:** AB4A6D4F6BF33EDA1425907A6AE94B571411E6536C99D23AB53F52CDF7071A4E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Secure Preferences	binary

PID	Process	Filename	Type
		MD5: 9E87939D19461A83683F525B3CF959B8 **SHA256:** 8BABC981574586EBD959E9B2CDDB3764B5D94AE90CE0788FF1A2BDB431233E13	
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865\manifest.fingerprint **MD5:** 1D09A9A5E62B846125CD7B929CCCBE44 **SHA256:** 1703E4E777B285ABA435E71256890A5FE92D24CB01E0EEFD03BADDCA228EEE2F	text
2152	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_966051865_metadata\verified_contents.json **MD5:** 117D173E82B282DECA740475E35C8ECD **SHA256:** 65491B21947D60C87C6358DCF69DF9ACA2B99E8F3B611BD3D559699BBC25000B	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\f6f122ba-b966-4a15-a6ee-fcb9795b2830.tmp **MD5:** 2800881C775077E1C4B6E06BF4676DE4 **SHA256:** 226EEC4486509917AA336AFEBD6FF65777B75B65F1FB06891D2A857A9421A974	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\Network Persistent State **MD5:** 2800881C775077E1C4B6E06BF4676DE4 **SHA256:** 226EEC4486509917AA336AFEBD6FF65777B75B65F1FB06891D2A857A9421A974	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\TransportSecurity **MD5:** 3794CF9C14B7E654295BA6DCCF4518AB **SHA256:** 46E2F0A382B3FF8EC94AB3847D9533C2D1E2F0FFFE90240F5597F0A33DC8908C	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Login Data For Account-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Affiliation Database-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\Database\LOG **MD5:** 4FA50A4821A50BA599BD4943D2F7ACF3 **SHA256:** 1BEF9633DD3EB3243E81099B3F8ADC7D5B9B32A145C61C641B9F5AA238FF5E41	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Web Data-journal **MD5:** — **SHA256:** —	—
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Safe Browsing Network\Safe Browsing Cookies-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Login Data-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\Database\000003.log **MD5:** C521BC75313FAB82F8986630D19444F1 **SHA256:** 7146B4A63320BF1A8E67449EA95A6B1DAAC25EB63A545997746B17976F40AD5B	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Scripts\LOG **MD5:** 9948596FBC941C898CB2DDE84E004119 **SHA256:** BCC907B481456C825F7C62B39A22D01D892A3D0517E00A302F3741B439C49913	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Extension Settings\memhbiihnoblfombkckdfmemihcnlihc\LOG **MD5:** 158F544BF304C459DA8A536CC802675F **SHA256:** —	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Top Sites **MD5:** D9F0B0474A300A011F68B46397F7D5A5 **SHA256:** 2B46A91579A5018DBA7CE0BA48922E2F2E4632DBC4C89018072865695543157 0	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Favicons-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Site Characteristics Database\000003.log **MD5:** 148079685E25097536785F4536AF014B **SHA256:** F096BC366A931FBA656BDCD77B24AF15A5F29FC53281A727C79F82C608ECFAB8	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Site Characteristics Database\LOG **MD5:** B6C7A0FA0062656948991BC124C98E60 **SHA256:** E3524742DEC65B47F7E303D5EE99AEB29DD9A59AC06F8C8DCFF65E714375E6FE	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Scripts\000003.log **MD5:** 41C7D1373DE8E7BD508C548A70910E51 **SHA256:** 99C59CBE7DB56D56A286485635E4467004641C6275E708887DD35728EB05109A	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Visited Links **MD5:** 09B854A237149B4B555B85A6D52C87A6 **SHA256:** 3B997713DE45782467628E04325CDF3B2637B50CDAD6932626A42EED12EAF374	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\PrivateAggregation-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Rules\LOG **MD5:** D745EDBCF7E24647198484D61A60ECF7 **SHA256:** D810EB2DAE65E8188AF67B6EB88B82CC2F9AEE2404ABF126E22DD195477F41BE	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sessions\Session_13385801333912590 **MD5:** E7ED8DC17F68ADF4322D9579AD8B880D **SHA256:** 1175ABAFC22E198382462D676600633603A97DCCB1F1B5DA210AA869B4C52C16	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\Trust Tokens-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension State\LOG **MD5:** D1E8164C25CD1C124259CA5047D8F831 **SHA256:** —	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension State\000003.log **MD5:** E952942B492DB39A75DD2669B98EBE74 **SHA256:** 14F92B911F9FE774720461EEC5BB4761AE6BFC9445C67E30BF624A8694B4B1DA	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\ScriptCache\index-dir\the-real-index~RF127ebd.TMP **MD5:** 7099556B67CEE084B3803E96967596B0 **SHA256:** CA6692459CB314DC4D8F2E339B788DAD0B2BC58B21E3E574D9238FFC5878A970	binary

PID	Process	Filename	Type
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Shared Dictionary\db-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\WebStorage\QuotaManager-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Login Data For Account **MD5:** DFD4F60ADC85FC874327517EFED62FF7 **SHA256:** C007DA2E5FD780008F28336940B427C3BFD509C72A40BFB7759592149FF3606E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Web Data **MD5:** D7C937F1D8132E92DF520BF44070E940 **SHA256:** 3B05248952A16EF2BA0B62BE18D6DFE131E0195C60C2881EEAA9ED7C137554EA	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Login Data **MD5:** DFD4F60ADC85FC874327517EFED62FF7 **SHA256:** C007DA2E5FD780008F28336940B427C3BFD509C72A40BFB7759592149FF3606E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network Action Predictor-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\DIPS-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sync Data\LevelDB\LOG **MD5:** 3A23D18A13C048299A1B9528FCFFE957 **SHA256:** 24AF81FCDAF287382CDFEC1B95DA5595C3256F2BF443BE4444CA185BED537E1B	text
3192	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Session Storage\000003.log **MD5:** E9B44D66AF5BF91166D6BCF570FA7DE7 **SHA256:** —	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Safe Browsing Network\Safe Browsing Cookies **MD5:** FEBE8B30C72B9ED5786AE265EBAF844A **SHA256:** 72D049174F8BB874A5DB67735CE76CAB400F25A72391EC557EF2720785B4C4AC	binary
3192	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Session Storage\LOG **MD5:** 1BD81CA9D03E237417315F75C7403D99 **SHA256:** B4D9F4CFD042E704B9CB659D74D3B0DF2062E6FCB6736996DAAC2B38B2CDA08B	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Favicons **MD5:** BABD43551F1B29EB82E221460676126A **SHA256:** 46B5ECADA4EDB2585F87953F7847AEFC938BE2404B9D9455C772B97295B7B1CB	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\heavy_ad_intervention_opt_out.db-journal **MD5:** — **SHA256:** —	—
3192	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Storage\leveldb\LOG **MD5:** 0FAE19D5509B439A2C1416A733F545A8 **SHA256:** 6AF06F4158F98E5A34238FE880F4B4C069BABC72AD210680276D255CC0837D87	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sync Data\LevelDB\000003.log **MD5:** B14764CD1BC1AA64A1F0551CD3682B81 **SHA256:** 8FF00D859349A3EA206706CDD3FA2762AE7C8EFE2FDD33A95A72FEE45AAC6BC4	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\296f4c91-c2f4-46ea-bd94-fab7e4af91d5.tmp **MD5:** 3794CF9C14B7E654295BA6DCCF4518AB **SHA256:** 46E2F0A382B3FF8EC94AB3847D9533C2D1E2F0FFFE90240F5597F0A33DC8908C	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\Cookies-journal **MD5:** — **SHA256:** —	—
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\Reporting and NEL-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\BrowsingTopicsSiteData-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Shortcuts-journal **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\PrivateAggregation **MD5:** ACF6736F1860F509DF093FDEF82F3163 **SHA256:** 1995D295FBDC4A993462B46676932EC3E0E9C8E9F3079F71D64A6D080FA677A0	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\fa372c62-7899-4731-ba95-b6e0991d5bd8.tmp **MD5:** 5BD5ED0FD31F9578D0E07D23D5D16D1A **SHA256:** —	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Shared Dictionary\db **MD5:** B581F0FF8F8AA3371AE47B48C95329E8 **SHA256:** F8E7CD835195E4EFF7855D20676484CA75F7E7E4FE5B13164FC926B365E1DEA0	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\InterestGroups-wal **MD5:** F73BED025F54427D603A5FDD02F9EA44 **SHA256:** 4E4FFB189688329B4F46AB43752262201BDBED2A0782A26D5EF0C53F60317463	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\SharedStorage **MD5:** B9263BBF24428AACA95D04D04F3AEB6F **SHA256:** 1FE8F6113488865C546D2FAA55B21482662CE4BE19D4F505EEEFA09BC3131489	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\InterestGroups **MD5:** 75103CAE6F82C7738513AF2058CE9DDF **SHA256:** D46A296B05C25C1DB8E2256632855BB682A83034A13560B2F5635BA51456FB30	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension Rules\000003.log **MD5:** 891A884B9FA2BFF4519F5F56D2A25D62 **SHA256:** E2610960C3757D1757F206C7B84378EFA22D86DCF161A98096A5F0E56E1A367E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\WebStorage\QuotaManager	binary

PID	Process	Filename	Type
		MD5: ADF7F601A9C07F80C625D1A113CD3E72 **SHA256:** A17E952DB379A348750530FC2D26EC430801984503D00696188F8339DE78F102	
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GCM Store\Encryption\LOG **MD5:** 5DBE82D0AF65AB9D3DA71944FFF3CDE1 **SHA256:** —	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\ClientCertificates\LOG.old **MD5:** — **SHA256:** —	—
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\Cookies **MD5:** 450C3245E2C4E559557E3F3F1F4EFD74 **SHA256:** —	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\PersistentOriginTrials\LOG.old **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Secure Preferences~RF127ebd.TMP **MD5:** 9E87939D19461A83683F525B3CF959B8 **SHA256:** 8BABC981574586EBD959E9B2CDDB3764B5D94AE90CE0788FF1A2BDB431233E13	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\bfd541dc-643c-4c50-b83f-b67f91b4945c.tmp **MD5:** F263430E5F3DB5698E0B6AB9841EBA96 **SHA256:** B40FC4C8C1946E749958FA36957CF153D8BCE0AB7023D60A3861359728DC9C33	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Preferences~RF127ecd.TMP **MD5:** 2FEFB23BCA5580606BA16A2DB319093C **SHA256:** 8F1DC9DEAFA8E374E371E19F97B7C4FDEDB5FAF91C16CA0DF242E6C2A1114A2C	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\Reporting and NEL **MD5:** F0C027C92D2F48101D9F65ADEA882117 **SHA256:** D21C42156ECD8E9B32292296AE0D602DC2A3F66374E9910F38C5B8F57FFEFB8A	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Segmentation Platform\SignalDB\LOG.old **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\discounts_db\LOG.old **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\parcel_tracking_db\LOG.old **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\metadata\000003.log **MD5:** 6FA73A189C5390C8D8D777F061DBFF66 **SHA256:** —	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\metadata\LOG **MD5:** 122FD174E254B21D9EAD1A5B74B1251C **SHA256:** 7A4F7EE234E958189F924CC0F01F89A7D3C4BFC51C46A590C5DFDA1903B0731E	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\LOG **MD5:** 497C203414E89FCFCF74DD0063C0684A **SHA256:** —	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\db9b7f3e-15c6-4e98-9fa9-d4244c46e68b.tmp **MD5:** 52AFB05C294C6625DBF6401881FA354B **SHA256:** —	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\Network Persistent State~RF127edd.TMP **MD5:** 2800881C775077E1C4B6E06BF4676DE4 **SHA256:** 226EEC4486509917AA336AFEBD6FF65777B75B65F1FB06891D2A857A9421A974	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\heavy_ad_intervention_opt_out.db **MD5:** 023FD485A16AEB668E5426A8060153A8 **SHA256:** 85C7910F5FF38BB2FDBF88D2D072E50C6EDDA1E774C04B21D19DCDEC158B3DA3	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\000003.log **MD5:** 4047ABADD37E0F2DC9C5B6D6316A9FBC **SHA256:** 5244EF5FC97E41D8527D4D42AEE6C665E727D170255345C072CA0D036585D9BD	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\commerce_subscription_db\LOG.old **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\LOG.old **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\optimization_guide_hint_cache_store\LOG.old **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\AutofillStrikeDatabase\LOG.old **MD5:** — **SHA256:** —	—
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF127fb7.TMP **MD5:** 22F34F3C8E6CACD4D7C97C65F67C82B6 **SHA256:** 85DA821899515CE243833A2E057C80FD43E545EAABF31C68B871D6AD19E14D93	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Shortcuts **MD5:** C135AEDA0EEFFC53BBF903913C861F3E **SHA256:** FF1398EDCFA0EA35375AFA95CD25BC086AF7CE25CBA4A85318EEBD1252E29B4F	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\0b15320b-7b77-4eda-a7b0-184b3919698f.tmp **MD5:** 5C40CA584CC11CD3DDFD604792233286 **SHA256:** 62DB5AA1F83CB7E2F35ED8340F929CA327106C01DE4114EC824BE8A1C9EC7833	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Download Service\EntryDB\LOG.old	—

PID	Process	Filename	Type
		MD5: — SHA256: —	
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sync Data\LevelDB\LOG.old MD5: 3A23D18A13C048299A1B9528FCFFE957 SHA256: —	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Site Characteristics Database\LOG.old MD5: B6C7A0FA0062656948991BC124C98E60 SHA256: E3524742DEC65B47F7E303D5EE99AEB29DD9A59AC06F8C8DCFF65E714375E6FE	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\a5d2d8af-bc0d-4bdb-bc10-6b856cce6b72.tmp MD5: 5058F1AF8388633F609CADB75A75DC9D SHA256: CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\metadata\LOG.old MD5: 122FD174E254B21D9EAD1A5B74B1251C SHA256: 7A4F7EE234E958189F924CC0F01F89A7D3C4BFC51C46A590C5DFDA1903B0731E	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension State\LOG.old MD5: D1E8164C25CD1C124259CA5047D8F831 SHA256: 9DD59814A10C8E5B7B5BDABE65BEC19FC5FE3BC797A9BDEA2CF8E0D516ABC110	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\Database\LOG.old MD5: 4FA50A4821A50BA599BD4943D2F7ACF3 SHA256: 1BEF9633DD3EB3243E81099B3F8ADC7D5B9B32A145C61C641B9F5AA238FF5E41	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\LOG.old MD5: 497C203414E89FCFCF74DD0063C0684A SHA256: —	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\d0f6fffc-7f3c-4898-94c6-daa0daad6d9f.tmp MD5: D751713988987E9331980363E24189CE SHA256: 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\SCT Auditing Pending Reports~RF128351.TMP MD5: D751713988987E9331980363E24189CE SHA256: 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\b485e9c2-031d-4cec-ad40-154f3b07ca90.tmp MD5: 3433CCF3E03FC35B634CD0627833B0AD SHA256: F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GCM Store\Encryption\LOG.old MD5: 5DBE82D0AF65AB9D3DA71944FFF3CDE1 SHA256: 9BF3A4FB74F95EF754158312600AE6FEA5D0325DE0E58458B592BC218EAE8CDD	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\trusted_vault.pb~RF12839f.TMP MD5: 3433CCF3E03FC35B634CD0627833B0AD SHA256: F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\0f95eb6f-9370-4c83-8e2e-3098bf9c80bc.tmp MD5: 5C49E766B451563987944A7958B67A91 SHA256: 5E3CB00DAA9B60CEF1E959A60BE06896BD9F1ABF7D175C57F216C40D64283465	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\46dfc530-e156-45e4-a560-f24338c037a2.tmp MD5: D751713988987E9331980363E24189CE SHA256: 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Translate Ranker Model MD5: 5C49E766B451563987944A7958B67A91 SHA256: 5E3CB00DAA9B60CEF1E959A60BE06896BD9F1ABF7D175C57F216C40D64283465	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\c3e0d12d-7a82-483d-a83e-c98fab37373a.tmp MD5: 5058F1AF8388633F609CADB75A75DC9D SHA256: CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_898898911\785a5e0a-14e8-4e78-9c63-cb718426f220.tmp MD5: AF8E621AC13ACB0A44D63EDCE4DBAFAA SHA256: C0289FDCD971B0DFBA34BA844F9A99B6C13780C527171823B2CD4926BCBE0490	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old MD5: — SHA256: —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old MD5: — SHA256: —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\BudgetDatabase\LOG.old MD5: — SHA256: —	—
8868	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_898898911\CRX_INSTALL\manifest.json MD5: 245E3B5D1A0B49FC98299B9D8050AA60 SHA256: FC560442B53C3DFF65D9F2A9D5007E335C6A1E79407851F669C2D64EB016C6A3	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\785a5e0a-14e8-4e78-9c63-cb718426f220.tmp MD5: AF8E621AC13ACB0A44D63EDCE4DBAFAA SHA256: C0289FDCD971B0DFBA34BA844F9A99B6C13780C527171823B2CD4926BCBE0490	binary
5500	msedge.exe	C:\Users\admin\AppData\Local\D3DSCache\f4d41c5d09ae781\F4EB2D6C-ED2B-4BDD-AD9D-F913287E6768.lock MD5: F49655F856ACB8884CC0ACE29216F511 SHA256: 7852FCE59C67DDF1D6B8B997EAA1ADFAC004A9F3A91C37295DE9223674011FBA	text
1852	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_898898911\CRX_INSTALL\bg.js MD5: 6ADC10DD97401B10229F53676CEC152D SHA256: 63B521B6ECBCE6826F89021048EEEDC46E1B00C3A80B81DA5C5819CF82C5F352	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Storage\leveldb\LOG.old MD5: 0FAE19D5509B439A2C1416A733F545A8 SHA256: —	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\7c947551-92e4-4a48-8f3e-293ca8b55446.tmp MD5: 26149E076CFBD70FEBF9750B95205F2A SHA256: —	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Local State~RF12a59e.TMP	binary

PID	Process	Filename	Type
		MD5: B3C8885668920A7A37C0CB4E8B59FC78 **SHA256:** —	
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\6aa46587-eb1b-4037-a1a7-3e2ce279c9d4.tmp **MD5:** B502451863EE98F72C50DA7C7097DEBE **SHA256:** CFA54DDFFAEA219227541B48F615DFE3FE88DCBC74AAC3A3A7C5C18D737DAA8E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\BrowsingTopicsState~RF128cf6.TMP **MD5:** 26149E076CFBD70FEBF9750B95205F2A **SHA256:** 7C5100042DE177EFA426459FC652A2D454A4EC1794DA08352765A97F05F922B0	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Session Storage\LOG.old **MD5:** 1BD81CA9D03E237417315F75C7403D99 **SHA256:** B4D9F4CFD042E704B9CB659D74D3B0DF2062E6FCB6736996DAAC2B38B2CDA08B	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\2379a4f7-8fe2-414a-98e9-f00f8f753643.tmp **MD5:** 63830385F0AB04A0760A9D12C121DDD6 **SHA256:** 95BAA46614712DD64F7CF4CE9FBBD4FCF58F04C443EADF3C4887814E81D7FD7F	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\TransportSecurity~RF12aaa0.TMP **MD5:** 3794CF9C14B7E654295BA6DCCF4518AB **SHA256:** 46E2F0A382B3FF8EC94AB3847D9533C2D1E2F0FFFE90240F5597F0A33DC8908C	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_000006 **MD5:** 2749599D0C760696078E0DD60CEAFB68 **SHA256:** B55B06AA049446C48B48F4C36C0588B290E292A12EAA394E6F4E9B95F6689152	compressed
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Preferences~RF12aa13.TMP **MD5:** F263430E5F3DB5698E0B6AB9841EBA96 **SHA256:** B40FC4C8C1946E749958FA36957CF153D8BCE0AB7023D60A3861359728DC9C33	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\8917f2d5-95c7-4071-9da1-7fae28a447d0.tmp **MD5:** 9B6FB3F6739944E78CB8E578E5C6F0E6 **SHA256:** 75C34684BA7075DE354954D60EF79FF8430FFE3F12A780D16EC6FCDD27440FF1	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_000005 **MD5:** AC461BAE403A036BCA20037EA1BB2922 **SHA256:** 5B76F54EA95B9739E253A21E3567CCDA91CC41960E9CC630E0F7F0EF1E1E1292	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Extension Settings\memhbiihnoblfombkckdfmemihcnlihc\LOG.old **MD5:** 158F544BF304C459DA8A536CC802675F **SHA256:** EE1FA9835811A3D11DA8139089E96C6BC4C97BB141F0B45863E5E43A946194B6	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_372633086\manifest.fingerprint **MD5:** 00766A21BEC3D2DCB091CFE346FB60DD **SHA256:** B63D4EE5DA0828A109E251CB149F6B0C6968C43714C65C136BE635D631D32E0D	text
5740	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_372633086\data.txt **MD5:** FD8717BAD7CD0F60163E7C2B05210AAA **SHA256:** D5FACEA6ED705EA08962D52A30EBF38F6D42AEA50A7AF21B103D0388B7DAE34A	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_000007 **MD5:** F82A5EFA0B4135EFB4DBF03345689BB0 **SHA256:** 9AB2F60C8785BF83DBE50EAF663DFE22EADC797C2FF753C09F6D013EECD64580	binary
5740	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping3956_372633086\manifest.json **MD5:** 8C32B9F390FCC4F061885661DBE797BD **SHA256:** 1431C36E66B4FC53CA74E9B10EA0213245631AD7543FEF183A8DD2720A5B4AB4	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\8690259fe68f782c_0 **MD5:** 6A0419CC616A4071637453DE0CE84091 **SHA256:** 3CA77849B8ED67A3148E51E0A7F246D48EF1EF631C0618C2AF6AC344E376DA75	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_000008 **MD5:** 60413257CF28F2E30D0B84B820BEF751 **SHA256:** 4B6BC279512E903CC86666FF2F7F5B2E2E2855B1608820D0C3A7D6C25DEA7915	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF12b137.TMP **MD5:** 305B26BB6CEFA1239179C5ACC67313AE **SHA256:** B9065C41F64E73F21C0E120488654E5A63918B9A3FF95DA3A9C1705C9B74485E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\717985e91c12dac6_0 **MD5:** 5D08353165F4DC6985149D540C26E890 **SHA256:** FD3D1A457D64E369C9DD080F65F76725169148FBB6EACEA51A85E23CC76A9647	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\e8f1faedddfd09da_0 **MD5:** 6FD21EE8B5E91C0FD9E6B8A241BB90A0 **SHA256:** 5104FB5B15D48578A6132E3B5E44AA9ABCBF191C265CBCDB5DED2247B7730CEE	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_00000b **MD5:** AAF0B4391702A44E1E8874904CBB0BBC **SHA256:** 5DAC4E0F4A55BF5F0372727A5E9552E029BBFEBA193989E180E2672D091F664B	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_00000a **MD5:** 4E45D9B292AA3AF886DDF0029A9D4776 **SHA256:** —	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\a4fe37cc841c1f31_0 **MD5:** 9607C6D954DCE0C89BDB5A84B8724684 **SHA256:** DDDDC998465064D57D88E908D52F9639B31CA87A30DBF27298C89B24B020E038	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\c60f8f4b-5f9a-40d5-8ea3-b3343c723e6a.tmp **MD5:** 51EB5E18A82453891F7B689AD8F5765C **SHA256:** F1D856C0434561DCE3D6C4046CE2238B972097A040366C66F7A44F02E355702B	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_000009 **MD5:** 683F4F7C102A57CDB3C451267EF24422 **SHA256:** CC505CB2756468C5A3B500EB182C2512EFE5869B9D8E8C2E3390465B2D583BE6	compressed
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\3b715ef7ddd8066d_0 **MD5:** 98EA19C029B48B999227BD3B5A742579 **SHA256:** CC4B197BE18F89CA832637ECD2CD15DED10C6E68A38CFB36B2BD60FAF477BABE	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\bacdeb2251eb6fb9_0 **MD5:** 53A00D3DE7783B28056328C3AADD8226 **SHA256:** 9D9919EE83AABFCA98F5812B9989B2E315C445E2705A9034E79E07153E83A49A	binary

PID	Process	Filename	Type
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_00000c **MD5:** 0DC52D5156E0E3423A20671F85112A3A **SHA256:** 55D8D47F45278ED4E61568932ABC7DBBF8111BFD5F815A5FF0B90120C238551F	compressed
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\33d5f6913257176f_0 **MD5:** 5CBC8BD2F18B95A2646FE9A0DBDE5B36 **SHA256:** F9DCA811CCB51CF3DC7AB99680B9836E97605E0A81A1AD305E4407EC26DE5245	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\2fb4fc4d0d0bb39a_0 **MD5:** 4E50094BF2A23B6CF1FF12A401D545B7 **SHA256:** 1B898BD610D1427320B87DB9372CF47379A2F00E0C5EF8A9E78F2AF87EFC8E29	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_00000d **MD5:** 8A9AB43FB704A286E2DF8450D21C7951 **SHA256:** 922AAF84867DA29BAF383E513C812CA7B19B7AF19DD27754578EABE28A178DE1	compressed
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\16276fe45f71c10c_0 **MD5:** F4E10A15F3FA4B141AE0A69667D18EE4 **SHA256:** —	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_00000e **MD5:** F61F0D4D0F968D5BBA39A84C76277E1A **SHA256:** 57147F08949ABABE7DEEF611435AE418475A693E3823769A25C2A39B6EAD9CCC	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Cache\Cache_Data\f_00000f **MD5:** 41F11AA2C5D9DDEB5FBE1B49B6077A87 **SHA256:** 751DC80067786F9B7785DC679757B0111B1864F277EC052021E9220872CDD0AD	compressed
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\f31cc9dd09f82d85_0 **MD5:** A6BD55D13F46F5A1DC7B9AE2F3D45738 **SHA256:** C966CA6CA55ACAC5C0DCA11CE67AE4488C437151375546C6AFC6787EF4D05FA5	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\6ba4e335a6cf0e65_0 **MD5:** 28A962FA5ED6D8AC5273066A32DFBCBF **SHA256:** 84360F0956CC5B0050DDEC9FC81C22793ADEE26C0C0B04A6D2CF081B26BAA904	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\b913978cee2710b9_0 **MD5:** 265E29301E0EE2D1D882F86464E5DA79 **SHA256:** 0B2FB730CBA792A791AB4648F85924C63D7443A1F10662B6FC6C3814825E10E5	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\2038578deadea5f5_0 **MD5:** CBB7E50AC6892F885581FA13380A8B7E **SHA256:** 0490276F4DDCF6B0632BCD78AB08EC5E9736D2E153A1631CD5A33DB85FC7AA9A	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\cd39eb8d-d9be-497d-826a-586c88a0534c.tmp **MD5:** 6648F38709C9C6F63847F5E2ED1C9A0D **SHA256:** 2D0A69696496C4200F18A19A15B5C525669C9C788A09BB65EF045BE057D5E42D	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\3b03fa77-55e1-4397-b940-ea6e7cfdc839.tmp **MD5:** C9C5186662ED211EBE11B2092115191C **SHA256:** 02FB70C1455AECD406EFBE644DB60522184B17BCCBE2004A96D28B9BBFAE81AB	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Local State~RF12d2b9.TMP **MD5:** 63830385F0AB04A0760A9D12C121DDD6 **SHA256:** 95BAA46614712DD64F7CF4CE9FBBD4FCF58F04C443EADF3C4887814E81D7FD7F	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\04e0cba4-a442-4b0a-9eb4-d07f82759800.tmp **MD5:** C1F7F0756F7A061EA4E735A116981BF4 **SHA256:** 64E814EA4C3E69B955E23E2481D0C694F6DEB870762EE13B74AE8D69C5B7A89B	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Preferences~RF12d2b9.TMP **MD5:** B502451863EE98F72C50DA7C7097DEBE **SHA256:** CFA54DDFFAEA219227541B48F615DFE3FE88DCBC74AAC3A3A7C5C18D737DAA8E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\optimization_guide_hint_cache_store\LOG.old~RF12e16f.TMP **MD5:** — **SHA256:** —	—
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\TransportSecurity~RF12d4ad.TMP **MD5:** 9B6FB3F6739944E78CB8E578E5C6F0E6 **SHA256:** 75C34684BA7075DE354954D60EF79FF8430FFE3F12A780D16EC6FCDD27440FF1	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\commerce_subscription_db\LOG.old~RF12e17f.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RF12e17f.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\LOG.old~RF12e17f.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\ClientCertificates\LOG.old~RF12e17f.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RF12e17f.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sessions\Session_13385801365290970 **MD5:** FD8CDDB7BA7E637B73C52483C3D41F2A **SHA256:** 58F284020C266F857DB0AEA79077BEFEB972DB3250410F69466F7F71D95E408F	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RF12e18e.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sessions\Tabs_13385801375387970 **MD5:** F99C07CB8F91D492438347F49369C295 **SHA256:** —	binary
3192	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Storage\leveldb\000003.log **MD5:** 110942043951C364CECA9790189338DD **SHA256:** —	binary

PID	Process	Filename	Type
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\b0ed4c0b-f265-4c93-8e3a-259efeafb15e.tmp **MD5:** 0754BD4E54928C07703321C4942DA17D **SHA256:** 7BABCD72044E75216DF5B860A5AECA7A336F750BC308206BC32C279F4AD5CE4E	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Code Cache\js\index-dir\the-real-index~RF12dd0a.TMP **MD5:** B5CAE43ED00F18C8B1C38405B24D7105 **SHA256:** E8C46BE1CAF8D4DBC9CD112F4A0B9B147CC66C37671E8F8CEE98EA16F984CCC2	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\discounts_db\LOG.old~RF12e19e.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\parcel_tracking_db\LOG.old~RF12e17f.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\PersistentOriginTrials\LOG.old~RF12e19e.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Preferences~RF12dd1a.TMP **MD5:** C9C5186662ED211EBE11B2092115191C **SHA256:** —	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\Network Persistent State~RF12dd29.TMP **MD5:** 52AFB05C294C6625DBF6401881FA354B **SHA256:** D5E8AAFEB370BE36DA279802CF3D2674A75568832F30FEC19ED84C7E472056E3	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\1c4d302f-d2bc-456b-bea7-7acb51f3679b.tmp **MD5:** DBA0AF8DBC954B758F68FB6D80B8CE55 **SHA256:** 0A63490E3E503596D3160EEF28C1AA889A4E7E45D973E81D883E1E3760E9F8E1	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\AutofillStrikeDatabase\LOG.old~RF12e1bd.TMP **MD5:** — **SHA256:** —	—
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Download Service\EntryDB\LOG.old~RF12e1cd.TMP **MD5:** — **SHA256:** —	—
896	onestart.exe	C:\Users\admin\AppData\Local\Temp\f728dbbc-2141-4e75-8621-edc5c96a554e.tmp **MD5:** 12CAF7572F5D362132F953FE120AA1E2 **SHA256:** AF2688E02A935F39E532916AAE2A7DC18E67E98547E45C7FA6BAA95A2F5202FD	image
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Service Worker\Database\LOG.old~RF12e17f.TMP **MD5:** 4FA50A4821A50BA599BD4943D2F7ACF3 **SHA256:** —	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\5e435192-e5aa-4fc6-9395-1c7988696647.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Site Characteristics Database\LOG.old~RF12e17f.TMP **MD5:** B6C7A0FA0062656948991BC124C98E60 **SHA256:** E3524742DEC65B47F7E303D5EE99AEB29DD9A59AC06F8C8DCFF65E714375E6FE	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Storage\leveldb\LOG.old~RF12e17f.TMP **MD5:** 0FAE19D5509B439A2C1416A733F545A8 **SHA256:** 6AF06F4158F98E5A34238FE880F4B4C069BABC72AD210680276D255CC0837D87	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\metadata\LOG.old~RF12e18e.TMP **MD5:** 122FD174E254B21D9EAD1A5B74B1251C **SHA256:** —	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Extension State\LOG.old~RF12e18e.TMP **MD5:** D1E8164C25CD1C124259CA5047D8F831 **SHA256:** 9DD59814A10C8E5B7B5BDABE65BEC19FC5FE3BC797A9BDEA2CF8E0D516ABC110	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Sync Data\LevelDB\LOG.old~RF12e18e.TMP **MD5:** 3A23D18A13C048299A1B9528FCFFE957 **SHA256:** 24AF81FCDAF287382CDFEC1B95DA5595C3256F2BF443BE4444CA185BED537E1B	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\shared_proto_db\LOG.old~RF12e18e.TMP **MD5:** 497C203414E89FCFCF74DD0063C0684A **SHA256:** —	text
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\GCM Store\Encryption\LOG.old~RF12e1bd.TMP **MD5:** 5DBE82D0AF65AB9D3DA71944FFF3CDE1 **SHA256:** 9BF3A4FB74F95EF754158312600AE6FEA5D0325DE0E58458B592BC218EAE8CDD	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\45ce0a7c-0489-4458-9271-617b13b7792b.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\ce3f8694-b762-4b8a-92f9-3ffd7773d203.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\SCT Auditing Pending Reports~RF12e1bd.TMP **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\SCT Auditing Pending Reports~RF12e1cd.TMP **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\009751c2-8548-416a-80e1-b0ccee0205ca.tmp **MD5:** 65A0204307447242EC9E90A65E58F462 **SHA256:** —	binary
9096	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_1663339386\CRX_INSTALL\manifest.json **MD5:** 245E3B5D1A0B49FC98299B9D8050AA60 **SHA256:** FC560442B53C3DFF65D9F2A9D5007E335C6A1E79407851F669C2D64EB016C6A3	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\f7cd7b4c-a886-473b-959d-6e3553f3f762.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
8352	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_1663339386\CRX_INSTALL\bg.js	text

PID	Process	Filename	Type
		MD5: 6ADC10DD97401B10229F53676CEC152D **SHA256:** 63B521B6ECBCE6826F89021048EEEDC46E1B00C3A80B81DA5C5819CF82C5F352	
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\dde6c26a-0eae-427b-86b5-a5181e3d581d.tmp **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\36e7e74d-6291-4848-801e-a587f506e41a.tmp **MD5:** AF8E621AC13ACB0A44D63EDCE4DBAFAA **SHA256:** C0289FDCD971B0DFBA34BA844F9A99B6C13780C527171823B2CD4926BCBE0490	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\trusted_vault.pb~RF12e20b.TMP **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1280_1663339386\36e7e74d-6291-4848-801e-a587f506e41a.tmp **MD5:** AF8E621AC13ACB0A44D63EDCE4DBAFAA **SHA256:** C0289FDCD971B0DFBA34BA844F9A99B6C13780C527171823B2CD4926BCBE0490	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF12e45d.TMP **MD5:** 5C40CA584CC11CD3DDFD604792233286 **SHA256:** 62DB5AA1F83CB7E2F35ED8340F929CA327106C01DE4114EC824BE8A1C9EC7833	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\2f8a2ee7-b244-4bcf-bedc-1c97bb5f7591.tmp **MD5:** 300586A74E7CD242D2536AE8B2D5F021 **SHA256:** —	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\bc8f6c58-29eb-480e-a4da-ed96fc0778e5.tmp **MD5:** 26149E076CFBD70FEBF9750B95205F2A **SHA256:** —	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\BrowsingTopicsState~RF12eb91.TMP **MD5:** 26149E076CFBD70FEBF9750B95205F2A **SHA256:** 7C5100042DE177EFA426459FC652A2D454A4EC1794DA08352765A97F05F922B0	binary
7320	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State~RF12efa8.TMP **MD5:** B4226B1CDAC90D8757EAC0B2849CA12B **SHA256:** FD1B98064191D407A4B5E8C4696B353AF63304E26095B2DE9762FF4AA216A144	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Local State~RF1303eb.TMP **MD5:** 6648F38709C9C6F63847F5E2ED1C9A0D **SHA256:** 2D0A69696496C4200F18A19A15B5C525669C9C788A09BB65EF045BE057D5E42D	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\3faaf478-98b0-4ad0-bd23-a87004de614e.tmp **MD5:** C3F506CA253E97061EE8CA05506D0A00 **SHA256:** 5D7AA31B05632D31FCF1FB0AE15FF6E7B1D1320D3BFC076BE55F64EC80BC164F	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\d0f01503-3254-458f-8307-8e69e5935db7.tmp **MD5:** 91A5E12BDE04AABA09FBEB4A9E593A63 **SHA256:** 5A98BC9A5DDE0547684D7E7015E9550FB92156856AA77BE60B7B2B2664B52D9C	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\f77cee57-e8a0-4a90-9dd9-1acc3ffd2fec.tmp **MD5:** 6F848CAF41F3F88071C4F36CC6865025 **SHA256:** 8A8BBCF31E43A57A93A62AA93A24A69955C5A084834886BC9DF4101CE4594E91	binary
4652	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Network\TransportSecurity~RF13092b.TMP **MD5:** C1F7F0756F7A061EA4E735A116981BF4 **SHA256:** 64E814EA4C3E69B955E23E2481D0C694F6DEB870762EE13B74AE8D69C5B7A89B	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Preferences~RF13088f.TMP **MD5:** 0754BD4E54928C07703321C4942DA17D **SHA256:** 7BABCD72044E75216DF5B860A5AECA7A336F750BC308206BC32C279F4AD5CE4E	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\b2d1240d-5375-4df2-8276-a2b1c5345e02.tmp **MD5:** 560F8D7DAF5DF971612F93E1FF3C1B85 **SHA256:** B2AF42C52D890369BD8D316A0A8880DD302786E97AADCD5E158117817D489744	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF13107e.TMP **MD5:** 65A0204307447242EC9E90A65E58F462 **SHA256:** B73876D7960412C3C0214BCAE638FC340DCC4669E67EC3D48BC91C5578A16B82	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\2e86454c-831e-4638-b250-599582dd2a6e.tmp **MD5:** 51EB5E18A82453891F7B689AD8F5765C **SHA256:** F1D856C0434561DCE3D6C4046CE2238B972097A040366C66F7A44F02E355702B	binary
3956	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF130a63.TMP **MD5:** 51EB5E18A82453891F7B689AD8F5765C **SHA256:** F1D856C0434561DCE3D6C4046CE2238B972097A040366C66F7A44F02E355702B	binary
1280	onestart.exe	C:\Users\admin\AppData\Local\OneStart.ai\OneStart\User Data\Default\Local Extension Settings\memhbiihnoblfombkckdfmemihcnlihc\MANIFEST-000001 **MD5:** 5AF87DFD673BA2115E2FCF5CFDB727AB **SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4	binary

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
37	201	210	87

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
8752	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3956	msedge.exe	GET	200	18.173.205.43:80	http://ocsps.ssl.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQg3SSkKA74hABkhmlBtJTz8w3hlAQU%2BWC71OPVNPa49QaAJadz20ZpqJ4CEEJLalPOx2YUHCpjsaUcQQQ%3D	unknown	—	—	whitelisted
8948	msiexec.exe	GET	200	143.204.98.59:80	http://resources.onestart.ai/onestart_installer_132.0.6834.116.exe	unknown	—	—	—
7624	backgroundTaskHost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAUZZSZEmI49Gjh0j13P68w%3D	unknown	—	—	whitelisted
7156	svchost.exe	HEAD	200	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/fb6dd03b-99d7-4cc8-a878-91c8e655c2d3?P1=1741792167&P2=404&P3=2&P4=Yb6iM%2fSinefyhYWgagb%2fYbGVQxcNya5yj9%2bqUkSeH1djezf%2fbkiSoVJSjbcPXw0kra4Gu5CMIJ%2bZU7ljYqJ4Og%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/fb6dd03b-99d7-4cc8-a878-91c8e655c2d3?P1=1741792167&P2=404&P3=2&P4=Yb6iM%2fSinefyhYWgagb%2fYbGVQxcNya5yj9%2bqUkSeH1djezf%2fbkiSoVJSjbcPXw0kra4Gu5CMIJ%2bZU7ljYqJ4Og%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/6ca9004c-2afd-40c0-a9b1-4fec460952e5?P1=1741792167&P2=404&P3=2&P4=iUw53bVDokdYeVe8GvzHWdmBMaTRRws6uNN%2f7pnErPitaYc8Ckn1UmY1G49YP8xwrOWuT4bhRKyDOZdWfTLmRQ%3d%3d	unknown	—	—	whitelisted
3956	msedge.exe	GET	200	18.173.205.43:80	http://ocsps.ssl.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSoEwb5tith0jIBy9frSyNGB1IsAAQUNr1J%2FzEs669qQP6ZwBbtuvxI3V8CEEhAwkRt2T9xBNbvBB%2BwDhI%3D	unknown	—	—	whitelisted
7156	svchost.exe	HEAD	200	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/6ca9004c-2afd-40c0-a9b1-4fec460952e5?P1=1741792167&P2=404&P3=2&P4=iUw53bVDokdYeVe8GvzHWdmBMaTRRws6uNN%2f7pnErPitaYc8Ckn1UmY1G49YP8xwrOWuT4bhRKyDOZdWfTLmRQ%3d%3d	unknown	—	—	whitelisted
8752	SIHClient.exe	GET	200	95.101.149.131:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	—	—	whitelisted
8880	backgroundTaskHost.exe	GET	200	2.23.77.188:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAUZZSZEmI49Gjh0j13P68w%3D	unknown	—	—	whitelisted
9004	BackgroundTransferHost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	—	—	whitelisted
6544	svchost.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
9076	onestart_installer.exe	POST	200	108.138.26.17:80	http://log.onestart.ai/	unknown	—	—	—
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/fb6dd03b-99d7-4cc8-a878-91c8e655c2d3?P1=1741792167&P2=404&P3=2&P4=Yb6iM%2fSinefyhYWgagb%2fYbGVQxcNya5yj9%2bqUkSeH1djezf%2fbkiSoVJSjbcPXw0kra4Gu5CMIJ%2bZU7ljYqJ4Og%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/6ca9004c-2afd-40c0-a9b1-4fec460952e5?P1=1741792167&P2=404&P3=2&P4=iUw53bVDokdYeVe8GvzHWdmBMaTRRws6uNN%2f7pnErPitaYc8Ckn1UmY1G49YP8xwrOWuT4bhRKyDOZdWfTLmRQ%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/6ca9004c-2afd-40c0-a9b1-4fec460952e5?P1=1741792167&P2=404&P3=2&P4=iUw53bVDokdYeVe8GvzHWdmBMaTRRws6uNN%2f7pnErPitaYc8Ckn1UmY1G49YP8xwrOWuT4bhRKyDOZdWfTLmRQ%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/6ca9004c-2afd-40c0-a9b1-4fec460952e5?P1=1741792167&P2=404&P3=2&P4=iUw53bVDokdYeVe8GvzHWdmBMaTRRws6uNN%2f7pnErPitaYc8Ckn1UmY1G49YP8xwrOWuT4bhRKyDOZdWfTLmRQ%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/6ca9004c-2afd-40c0-a9b1-4fec460952e5?P1=1741792167&P2=404&P3=2&P4=iUw53bVDokdYeVe8GvzHWdmBMaTRRws6uNN%2f7pnErPitaYc8Ckn1UmY1G49YP8xwrOWuT4bhRKyDOZdWfTLmRQ%3d%3d	unknown	—	—	whitelisted

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/6ca9004c-2afd-40c0-a9b1-4fec460952e5?P1=1741792167&P2=404&P3=2&P4=iUw53bVDokdYeVe8GvzHWdmBMaTRRws6uNN%2f7pnErPitaYc8Ckn1UmY1G49YP8xwrOWuT4bhRKyDOZdWfTLmRQ%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/68591036-2289-4858-9f7f-9149e89c8a08?P1=1741788566&P2=404&P3=2&P4=Zm395UEjTkc4q4OGGovxcUMoGZc8vTaXlKYjeIxbCMF%2fmWVQWAvmVV8ieZdDUKBzc0E7%2ffqPHgXE0j%2fwMrrauw%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	HEAD	200	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/68591036-2289-4858-9f7f-9149e89c8a08?P1=1741788566&P2=404&P3=2&P4=Zm395UEjTkc4q4OGGovxcUMoGZc8vTaXlKYjeIxbCMF%2fmWVQWAvmVV8ieZdDUKBzc0E7%2ffqPHgXE0j%2fwMrrauw%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/68591036-2289-4858-9f7f-9149e89c8a08?P1=1741788566&P2=404&P3=2&P4=Zm395UEjTkc4q4OGGovxcUMoGZc8vTaXlKYjeIxbCMF%2fmWVQWAvmVV8ieZdDUKBzc0E7%2ffqPHgXE0j%2fwMrrauw%3d%3d	unknown	—	—	whitelisted
2924	SearchApp.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEA77flR%2B3w%2FxBpruV2lte6A%3D	unknown	—	—	whitelisted
2924	SearchApp.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	—	—	whitelisted
9076	onestart_installer.exe	POST	200	108.138.26.3:80	http://log.onestart.ai/	unknown	—	—	—
7156	svchost.exe	GET	206	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/68591036-2289-4858-9f7f-9149e89c8a08?P1=1741788566&P2=404&P3=2&P4=Zm395UEjTkc4q4OGGovxcUMoGZc8vTaXlKYjeIxbCMF%2fmWVQWAvmVV8ieZdDUKBzc0E7%2ffqPHgXE0j%2fwMrrauw%3d%3d	unknown	—	—	whitelisted
3012	onestart.exe	POST	200	108.138.26.3:80	http://log.onestart.ai/	unknown	—	—	—
4652	onestart.exe	GET	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/mfnf4w4aaa2rporuqgtjqv35v4_4.10.2891.0/oimompecagnajdejgnnjijobebaeigek_4.10.2891.0_win64_acwxtxt2znguar3w2o252umtomsq.crx3	unknown	—	—	whitelisted
1280	onestart.exe	POST	200	108.138.26.3:80	http://log.onestart.ai/	unknown	—	—	—
2924	SearchApp.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHl3O1J0%3D	unknown	—	—	whitelisted
7156	svchost.exe	HEAD	200	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/pkap37pjanhqytozbeza7qsifm_2025.2.21.0/niikhdgajlphfehepabhhblakbdgeefj_2025.02.21.00_all_d4p2fl3zreu7j7izvavx2icubq.crx3	unknown	—	—	whitelisted
7156	svchost.exe	HEAD	200	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/f28d972a-574d-41b9-8559-4ab486e8a4f0?P1=1741788569&P2=404&P3=2&P4=IjU7VAAbCp2QR%2ffnBFq9IZXzF2WGkcXd3rOqTVRH%2ftXa538ka8kJvwp7s%2bd7VsnP9s9f%2fudjlAMwsFyGYtUO6A%3d%3d	unknown	—	—	whitelisted
2924	SearchApp.exe	GET	200	184.30.131.245:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/pkap37pjanhqytozbeza7qsifm_2025.2.21.0/niikhdgajlphfehepabhhblakbdgeefj_2025.02.21.00_all_d4p2fl3zreu7j7izvavx2icubq.crx3	unknown	—	—	whitelisted
7156	svchost.exe	GET	200	199.232.210.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/f28d972a-574d-41b9-8559-4ab486e8a4f0?P1=1741788569&P2=404&P3=2&P4=IjU7VAAbCp2QR%2ffnBFq9IZXzF2WGkcXd3rOqTVRH%2ftXa538ka8kJvwp7s%2bd7VsnP9s9f%2fudjlAMwsFyGYtUO6A%3d%3d	unknown	—	—	whitelisted
7156	svchost.exe	GET	206	34.104.35.123:80	http://edgedl.me.gvt1.com/edgedl/release2/chrome_component/pkap37pjanhqytozbeza7qsifm_2025.2.21.0/niikhdgajlphfehepabhhblakbdgeefj_2025.02.21.00_all_d4p2fl3zreu7j7izvavx2icubq.crx3	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2104	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:137	—	—	—	whitelisted
—	—	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
7320	msedge.exe	18.245.60.105:80	smartonestartpdf.com	—	US	unknown
3956	msedge.exe	239.255.255.250:1900	—	—	—	whitelisted
7320	msedge.exe	142.250.185.163:443	fonts.gstatic.com	—	—	whitelisted
7320	msedge.exe	142.250.186.42:443	fonts.googleapis.com	GOOGLE	US	whitelisted
7320	msedge.exe	13.107.42.16:443	config.edge.skype.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	13.107.21.239:443	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	18.245.60.105:443	smartonestartpdf.com	—	US	unknown
7320	msedge.exe	13.107.6.158:443	business.bing.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	13.107.246.44:443	edge-mobile-static.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	23.48.23.26:443	bzib.nelreports.net	Akamai International B.V.	DE	whitelisted
7320	msedge.exe	2.16.110.171:443	www.bing.com	Akamai International B.V.	DE	whitelisted
7320	msedge.exe	104.18.31.234:443	app.termly.io	CLOUDFLARENET	—	suspicious
7320	msedge.exe	18.245.60.33:443	smartonestartpdf.com	—	US	unknown
7320	msedge.exe	13.107.253.44:443	xpaywalletcdn.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	172.217.16.200:443	www.googletagmanager.com	GOOGLE	US	whitelisted
7320	msedge.exe	143.204.98.36:443	res.smartonestartpdf.com	AMAZON-02	US	unknown
7320	msedge.exe	216.239.36.181:443	analytics.google.com	GOOGLE	US	whitelisted
7320	msedge.exe	74.125.133.155:443	stats.g.doubleclick.net	GOOGLE	US	whitelisted
3216	svchost.exe	40.113.103.199:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
7320	msedge.exe	3.161.82.7:443	northlightconnect.net	—	US	unknown
6544	svchost.exe	40.126.31.73:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6544	svchost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
2112	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
7320	msedge.exe	142.250.186.131:443	update.googleapis.com	GOOGLE	US	whitelisted
7320	msedge.exe	142.250.186.129:443	clients2.googleusercontent.com	GOOGLE	US	whitelisted
7320	msedge.exe	204.79.197.239:443	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7624	backgroundTaskHost.exe	20.223.36.55:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
3956	msedge.exe	224.0.0.251:5353	—	—	—	unknown
7624	backgroundTaskHost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
9004	BackgroundTransferHost.exe	2.16.110.171:443	www.bing.com	Akamai International B.V.	DE	whitelisted
3956	msedge.exe	18.173.205.43:80	ocsps.ssl.com	—	US	whitelisted
2104	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
9004	BackgroundTransferHost.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
8752	SIHClient.exe	4.245.163.56:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
8752	SIHClient.exe	95.101.149.131:80	www.microsoft.com	Akamai International B.V.	NL	whitelisted
8752	SIHClient.exe	20.242.39.171:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	13.107.253.72:443	edge-consumer-static.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	204.79.197.203:443	ntp.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

PID	Process	IP	Domain	ASN	CN	Reputation
7320	msedge.exe	95.101.182.24:443	assets.msn.com	Akamai International B.V.	FR	whitelisted
7320	msedge.exe	13.74.129.1:443	c.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
7320	msedge.exe	184.86.251.21:443	www.bing.com	Akamai International B.V.	DE	whitelisted
7320	msedge.exe	150.171.27.10:443	c.bing.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	13.89.179.11:443	browser.events.data.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	184.86.251.9:443	th.bing.com	Akamai International B.V.	DE	whitelisted
7320	msedge.exe	18.244.18.38:443	sb.scorecardresearch.com	—	US	whitelisted
7320	msedge.exe	2.16.164.64:443	img-s-msn-com.akamaized.net	Akamai International B.V.	NL	whitelisted
7320	msedge.exe	92.123.20.182:443	ecn.dev.virtualearth.net	AKAMAI-AS	AT	whitelisted
7320	msedge.exe	13.107.42.14:443	px.ads.linkedin.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7320	msedge.exe	2.23.227.208:443	r.bing.com	Ooredoo Q.S.C.	QA	whitelisted
7320	msedge.exe	204.79.197.219:443	r.msftstatic.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
8360	svchost.exe	2.19.246.123:443	go.microsoft.com	AKAMAI-AS	DE	whitelisted
8948	msiexec.exe	143.204.98.59:80	resources.onestart.ai	AMAZON-02	US	suspicious
8880	backgroundTaskHost.exe	20.199.58.43:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
8880	backgroundTaskHost.exe	2.23.77.188:80	ocsp.digicert.com	AKAMAI-AS	DE	whitelisted
8880	backgroundTaskHost.exe	20.223.35.26:443	fd.api.iris.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
7320	msedge.exe	2.19.246.123:443	go.microsoft.com	AKAMAI-AS	DE	whitelisted
7320	msedge.exe	2.16.164.130:443	deff.nelreports.net	Akamai International B.V.	NL	whitelisted
3812	svchost.exe	239.255.255.250:1900	—	—	—	whitelisted
7156	svchost.exe	199.232.210.172:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	FASTLY	US	whitelisted
7900	slui.exe	40.91.76.224:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
9076	onestart_installer.exe	13.33.187.71:443	onestart.ai	—	US	suspicious
9076	onestart_installer.exe	108.138.26.17:80	log.onestart.ai	AMAZON-02	US	suspicious
9076	onestart_installer.exe	108.138.26.3:80	log.onestart.ai	AMAZON-02	US	suspicious
4652	onestart.exe	142.250.185.227:443	update.googleapis.com	GOOGLE	US	whitelisted
3012	onestart.exe	13.33.187.71:443	onestart.ai	—	US	suspicious
3012	onestart.exe	99.86.4.6:443	api.onestart.ai	AMAZON-02	US	suspicious
3012	onestart.exe	99.86.4.13:443	api.onestart.ai	AMAZON-02	US	suspicious
1280	onestart.exe	13.33.187.71:443	onestart.ai	—	US	suspicious
3012	onestart.exe	108.138.26.3:80	log.onestart.ai	AMAZON-02	US	suspicious
4652	onestart.exe	34.104.35.123:80	edgedl.me.gvt1.com	GOOGLE	US	whitelisted
4652	onestart.exe	13.33.187.71:443	onestart.ai	—	US	suspicious
4652	onestart.exe	173.194.69.84:443	accounts.google.com	GOOGLE	US	whitelisted
4652	onestart.exe	13.33.187.77:443	onestart.ai	—	US	suspicious
4652	onestart.exe	142.250.184.196:443	www.google.com	GOOGLE	US	whitelisted
4652	onestart.exe	142.250.185.67:443	www.gstatic.com	GOOGLE	US	whitelisted
4652	onestart.exe	142.250.184.202:443	ogads-pa.googleapis.com	GOOGLE	US	whitelisted
4652	onestart.exe	142.250.185.78:443	apis.google.com	GOOGLE	US	whitelisted
4652	onestart.exe	142.250.185.174:443	play.google.com	—	—	whitelisted
4652	onestart.exe	172.217.16.206:443	chrome.google.com	GOOGLE	US	whitelisted
4652	onestart.exe	13.33.187.4:443	onestart.ai	—	US	suspicious

PID	Process	IP	Domain	ASN	CN	Reputation
4652	onestart.exe	142.250.185.202:443	ogads-pa.googleapis.com	GOOGLE	US	whitelisted
1280	onestart.exe	108.138.26.3:80	log.onestart.ai	AMAZON-02	US	suspicious
2924	SearchApp.exe	2.16.110.121:443	www.bing.com	Akamai International B.V.	DE	whitelisted
2924	SearchApp.exe	2.16.110.176:443	www.bing.com	Akamai International B.V.	DE	whitelisted
2924	SearchApp.exe	184.30.131.245:80	ocsp.digicert.com	AKAMAI-AS	US	whitelisted
2924	SearchApp.exe	150.171.27.10:443	c.bing.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2924	SearchApp.exe	204.79.197.222:443	fp.msedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7744	slui.exe	40.91.76.224:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2924	SearchApp.exe	150.171.70.254:443	mcr-ring.msedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
4652	onestart.exe	13.33.187.25:443	onestart.ai	—	US	suspicious
2924	SearchApp.exe	13.107.49.254:443	q-ring.msedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2924	SearchApp.exe	13.107.42.14:443	px.ads.linkedin.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4652	onestart.exe	142.250.186.46:80	google.com	GOOGLE	US	whitelisted
4652	onestart.exe	142.250.186.46:443	google.com	GOOGLE	US	whitelisted
4652	onestart.exe	142.250.185.106:443	ogads-pa.googleapis.com	GOOGLE	US	whitelisted
4652	onestart.exe	172.217.16.131:443	fonts.gstatic.com	—	—	whitelisted
4652	onestart.exe	216.58.206.74:443	ogads-pa.googleapis.com	—	—	whitelisted
4652	onestart.exe	142.250.186.131:443	update.googleapis.com	GOOGLE	US	whitelisted
4652	onestart.exe	216.58.206.42:443	ogads-pa.googleapis.com	—	—	whitelisted
7156	svchost.exe	34.104.35.123:80	edgedl.me.gvt1.com	GOOGLE	US	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	40.127.240.158 20.73.194.208	whitelisted
google.com	142.250.186.142 142.250.186.46	whitelisted
config.edge.skype.com	13.107.42.16	whitelisted
smartonestartpdf.com	18.245.60.105 18.245.60.60 18.245.60.122 18.245.60.33	unknown
edge.microsoft.com	13.107.21.239 204.79.197.239	whitelisted
business.bing.com	13.107.6.158	whitelisted
edge-mobile-static.azureedge.net	13.107.246.44	whitelisted
bzib.nelreports.net	23.48.23.26 23.48.23.51	whitelisted
www.bing.com	2.16.110.171 2.16.110.121 2.16.110.123 184.86.251.21 184.86.251.30 184.86.251.28 184.86.251.15 184.86.251.25 184.86.251.27 184.86.251.16 184.86.251.24 184.86.251.14 2.17.22.17 2.17.22.34 2.17.22.65	whitelisted

Domain	IP	Reputation
	2.17.22.43 2.17.22.42 95.101.79.80 2.17.22.59 2.17.22.67 2.17.22.25 2.16.110.176	
app.termly.io	104.18.31.234 104.18.30.234	unknown
fonts.googleapis.com	142.250.186.42	whitelisted
fonts.gstatic.com	142.250.185.163 172.217.16.131	whitelisted
xpaywalletcdn.azureedge.net	13.107.253.44	whitelisted
res.smartonestartpdf.com	143.204.98.36 143.204.98.39 143.204.98.61 143.204.98.124	unknown
www.googletagmanager.com	172.217.16.200	whitelisted
analytics.google.com	216.239.36.181 216.239.34.181 216.239.32.181 216.239.38.181	whitelisted
stats.g.doubleclick.net	74.125.133.155 74.125.133.156 74.125.133.154 74.125.133.157	whitelisted
northlightconnect.net	3.161.82.7 3.161.82.108 3.161.82.26 3.161.82.39	unknown
client.wns.windows.com	40.113.103.199	whitelisted
login.live.com	40.126.31.73 20.190.159.130 40.126.31.67 40.126.31.71 20.190.159.75 20.190.159.71 40.126.31.69 20.190.159.64	whitelisted
ocsp.digicert.com	184.30.131.245 2.23.77.188	whitelisted
update.googleapis.com	142.250.186.131 142.250.185.227	whitelisted
edgeservices.bing.com	2.16.110.171 2.16.110.123 2.16.110.121	whitelisted
clients2.googleusercontent.com	142.250.186.129	whitelisted
edgeassetservice.azureedge.net	13.107.246.44	whitelisted
arc.msn.com	20.223.36.55 20.199.58.43	whitelisted
ocsps.ssl.com	18.173.205.43 18.173.205.113 18.173.205.76 18.173.205.57	whitelisted
slscr.update.microsoft.com	4.245.163.56	whitelisted
www.microsoft.com	95.101.149.131	whitelisted
fe3cr.delivery.mp.microsoft.com	20.242.39.171	whitelisted
edge-consumer-static.azureedge.net	13.107.253.72	whitelisted
ntp.msn.com	204.79.197.203	whitelisted
img-s-msn-com.akamaized.net	2.16.164.64 2.16.164.16	whitelisted

Domain	IP	Reputation
sb.scorecardresearch.com	18.244.18.38 18.244.18.32 18.244.18.27 18.244.18.122	whitelisted
th.bing.com	184.86.251.9 184.86.251.16 184.86.251.10 184.86.251.13 184.86.251.14 184.86.251.15 184.86.251.12 184.86.251.8 184.86.251.11 2.16.110.176 2.16.110.121 2.16.110.171 2.16.110.123	whitelisted
assets.msn.com	95.101.182.24 95.101.182.65 95.101.182.16 95.101.182.64 95.101.182.11 95.101.182.59 95.101.182.9 95.101.182.35 95.101.182.58	whitelisted
c.msn.com	13.74.129.1	whitelisted
c.bing.com	150.171.27.10 150.171.28.10	whitelisted
api.msn.com	204.79.197.203	whitelisted
browser.events.data.msn.com	13.89.179.11	whitelisted
ecn.dev.virtualearth.net	92.123.20.182	whitelisted
srtb.msn.com	204.79.197.203	whitelisted
px.ads.linkedin.com	13.107.42.14	whitelisted
r.bing.com	2.23.227.208 2.23.227.215	whitelisted
r.msftstatic.com	204.79.197.219	whitelisted
go.microsoft.com	2.19.246.123	whitelisted
resources.onestart.ai	143.204.98.59 143.204.98.8 143.204.98.32 143.204.98.82	unknown
fd.api.iris.microsoft.com	20.223.35.26	whitelisted
deff.nelreports.net	2.16.164.130 2.16.164.48	whitelisted
msedge.b.tlu.dl.delivery.mp.microsoft.com	199.232.210.172 199.232.214.172 217.20.57.36 84.201.210.23 217.20.57.35 84.201.210.39 217.20.57.34 217.20.57.19 217.20.57.20 217.20.57.18	whitelisted
activation-v2.sls.microsoft.com	40.91.76.224	whitelisted
nexusrules.officeapps.live.com	52.111.236.22	whitelisted
onestart.ai	13.33.187.71 13.33.187.25 13.33.187.4 13.33.187.77	unknown
log.onestart.ai	108.138.26.17 108.138.26.115 108.138.26.3	unknown

Domain	IP	Reputation
	108.138.26.36	
api.onestart.ai	99.86.4.6 99.86.4.83 99.86.4.65 99.86.4.13	unknown
api2.onestart.ai	99.86.4.13 99.86.4.6 99.86.4.65 99.86.4.83	unknown
edgedl.me.gvt1.com	34.104.35.123	whitelisted
accounts.google.com	173.194.69.84	whitelisted
www.google.com	142.250.184.196	whitelisted
www.gstatic.com	142.250.185.67	whitelisted
ogads-pa.googleapis.com	142.250.184.202 142.250.185.170 172.217.16.138 142.250.186.170 142.250.181.234 216.58.212.138 142.250.185.234 142.250.185.202 142.250.185.106 172.217.18.10 216.58.206.42 172.217.23.106 142.250.184.234 142.250.185.74 142.250.185.138 216.58.206.74	whitelisted
apis.google.com	142.250.185.78	whitelisted
play.google.com	142.250.185.174	whitelisted
chrome.google.com	172.217.16.206	whitelisted
optimizationguide-pa.googleapis.com	142.250.185.202 142.250.186.74 172.217.16.202 216.58.212.170 142.250.185.234 142.250.185.170 142.250.181.234 142.250.186.106 142.250.186.170 142.250.185.138 142.250.186.138 142.250.185.106 142.250.185.74 216.58.212.138 142.250.186.42 216.58.206.42	whitelisted
www2.bing.com	150.171.27.10 150.171.28.10	whitelisted
fp.msedge.net	204.79.197.222	whitelisted
mcr-ring.msedge.net	150.171.70.254 150.171.69.254	unknown
q-ring.msedge.net	13.107.49.254	whitelisted
rum14.perf.linkedin.com	13.107.42.14	whitelisted
content-autofill.googleapis.com	142.250.185.106 142.250.185.170 172.217.18.106 142.250.181.234 142.250.185.234 142.250.185.202 216.58.206.74 172.217.16.138 142.250.184.234 142.250.185.74 172.217.18.10	whitelisted

Domain	IP	Reputation
	142.250.185.138 142.250.184.202 216.58.212.138 172.217.23.106 142.250.186.170	
ogs.google.com	172.217.16.206	whitelisted
ssl.gstatic.com	142.250.186.131	whitelisted

Threats

PID	Process	Class	Message
–	–	Possibly Unwanted Program Detected	ADWARE [ANY.RUN] AdvancedInstaller User-Agent
–	–	Potential Corporate Privacy Violation	ET INFO PE EXE or DLL Windows file download HTTP
–	–	Potentially Bad Traffic	ET INFO Executable served from Amazon S3
–	–	Possibly Unwanted Program Detected	ET ADWARE_PUP Onestart AI Program Version Checkin (POST)
–	–	Possibly Unwanted Program Detected	ET ADWARE_PUP Onestart AI Program Version Checkin (POST)
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Possibly Unwanted Program Detected	ET ADWARE_PUP Onestart AI Host Profile Checkin (POST)
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt

PID	Process	Class	Message
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt

PID	Process	Class	Message
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt
–	–	Generic Protocol Command Decode	SURICATA QUIC failed decrypt

Debug output strings

No debug info

ANY RUN INTERACTIVE MALWARE ANALYSIS

Interactive malware hunting service ANY.RUN
© 2017-2025 ANY.RUN LLC. ALL RIGHTS RESERVED