ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

URL: https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fzntsfboczi.rd.klockars.com%2F4HLNCy3713Lzgc273iqwcbcyxtq146KUKCHPYUBZWBTFM394829SAJX1570z1&data=05%7C02%7C%7C28c54cb9ea4f419d216d08ddfacceeed%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C638942480313925508%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=lhZPq8qVu0rhAC9xFvggHdl8eG0MdNDtPfAyWh1unHg%3D&reserved=0

Full analysis: https://app.any.run/tasks/2b424966-ecdf-4276-b4f7-1116ed1a167e

Verdict: Malicious activity

Analysis date: September 23, 2025 at 21:40:23

OS: Windows 10 Professional (build: 19044, 64 bit)

Tags: evil-redirect | phishing | foxwhoops

Indicators:

MD5: 8CD7A169656FA1C34981E89A90C0B79C

SHA1: 6358903F51BC9ECADCB2419984696C98330F8676

SHA256: 216786186F382129D46519D59E274273AAFB8EC8131D931ED270D75FE19460F6

SSDEEP: 12:2lqVsJLDcnXH8RVilXBBtEyWwKuN1SiZPpD/:2lqAL8sziuBth3RN1Sc

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	**Heavy Evasion option:**	off	**Network geolocation:**	off
Additional time used:	none	**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 (133.0.6943.127)
- 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 (133.0.3065.92)
- 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) (136.0)
- Mozilla Maintenance Service (136.0)
- 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)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)

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

- 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)

Behavior activities

MALICIOUS

PHISHING has been detected (SURICATA)
- msedge.exe (PID: 1944)

SUSPICIOUS

No suspicious indicators.

INFO

Checks supported languages
- identity_helper.exe (PID: 7876)

Application launched itself
- msedge.exe (PID: 2508)

Reads Environment values
- identity_helper.exe (PID: 7876)

Reads the computer name
- identity_helper.exe (PID: 7876)

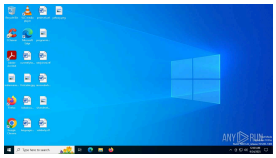
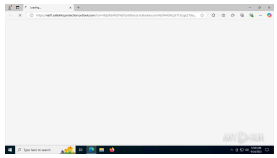
Malware configuration

No Malware configuration.

Static information

No data.

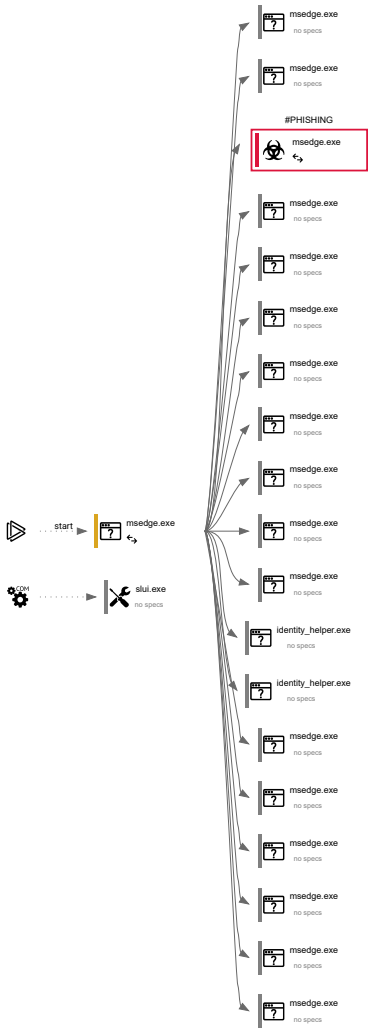
Video and screenshots

Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
157	21	1	1

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
856	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --video-capture-use-gpu-memory-buffer --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 --always-read-main-dll --field-trial-handle=3628,i,14124658337064150998,1648727050267243842,262144 --variations-seed-version --mojo-platform-channel-handle=3640 /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:	133.0.3065.92		

1028	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --extension-process --renderer-sub-type=extension --video-capture-use-gpu-memory-buffer --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 --always-read-main-dll --field-trial-handle=4336,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=4360 /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:**	133.0.3065.92

1132	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --disable-quic --string-annotations --always-read-main-dll --field-trial-handle=2748,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=2768 /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:	133.0.3065.92		

1324	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --disable-quic --message-loop-type-ui --string-annotations --always-read-main-dll --field-trial-handle=6600,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=1504 /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:**	133.0.3065.92

1808	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --disable-quic --message-loop-type-ui --string-annotations --always-read-main-dll --field-trial-handle=6336,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=1464 /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:**	133.0.3065.92

1944	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --always-read-main-dll --field-trial-handle=2252,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=2556 /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:	133.0.3065.92		

2508	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" "https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fzntsfboczi.rd.klockars.com%2F4HLNCy3713Lzgc273iqwcbcyxtq146KUKCHPYUBZWBTFM394829SAJX1570z1&data=05%7C02%7C%7C28c54cb9ea4f419d216d08ddfacceeed%7C84df9e7fe9f640afb435aaaaaaaaaaaa%7C1%7C0%7C638942480313925508%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=IhZPq8qVu0rhAC9xFvggHdl8eG0MdNDtPfAyWh1unHg%3D&reserved=0"	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	↪	explorer.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

3584	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --string-annotations --gpu-preferences=UAAAAAAAADgAAAEAAAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAAAAA --always-read-main-dll --field-trial-handle=2412,i,14124658337064150998,1648727050267243842,262144 --variations-seed-version --mojo-platform-channel-handle=2400 /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:	133.0.3065.92		

4072	"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=133.0.6943.142 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 --annotation=prod=Edge --annotation=ver=133.0.3065.92 --initial-client-data=0x304,0x308,0x30c,0x2fc,0x314,0x7ffc4442f208,0x7ffc4442f214,0x7ffc4442f220	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Version:	133.0.3065.92		

4884	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --video-capture-use-gpu-memory-buffer --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 --always-read-main-dll --field-trial-handle=3656,i,14124658337064150998,1648727050267243842,262144 --variations-seed-version --mojo-platform-channel-handle=3696 /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:**	133.0.3065.92

7504	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=8 --always-read-main-dll --field-trial-handle=5324,i,14124658337064150998,1648727050267243842,262144 --variations-seed-version --mojo-platform-channel-handle=5336 /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:**	133.0.3065.92

7512	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --disable-quic --message-loop-type-ui --string-annotations --always-read-main-dll --field-trial-handle=6312,i,14124658337064150998,1648727050267243842,262144 --variations-seed-version --mojo-platform-channel-handle=1488 /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:**	133.0.3065.92

7536	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --disable-gpu-compositing --video-capture-use-gpu-memory-buffer --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 --always-read-main-dll --field-trial-handle=5512,i,14124658337064150998,1648727050267243842,262144 --variations-seed-version --mojo-platform-channel-handle=4540 /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

	User: admin	Company: Microsoft Corporation			
7760	Integrity Level: LOW Version: 133.0.3065.92	Description: Microsoft Edge	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store_service.mojom.AssetStoreService --lang=en-US --service-sandbox-type=asset_store_service --disable-quic --string-annotations --always-read-main-dll --field-trial-handle=5348,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=5628 /prefetch:8

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	LOW	Description:	Microsoft Edge
Exit code:	0	Version:	133.0.3065.92

7768	"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 --disable-quic --onnx-enabled-for-ee --string-annotations --always-read-main-dll --field-trial-handle=5540,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=5684 /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:	133.0.3065.92

7864	"C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --always-read-main-dll --field-trial-handle=6168,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=6220 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\identity_helper.exe	–	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	PWA Identity Proxy Host
Exit code:	3221226029	Version:	133.0.3065.92

7876	"C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --disable-quic --string-annotations --always-read-main-dll --field-trial-handle=6168,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=6220 /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.92\identity_helper.exe	–	msedge.exe

Information

User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	PWA Identity Proxy Host
Exit code:	0	Version:	133.0.3065.92

7888	"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 --disable-quic --string-annotations --always-read-main-dll --field-trial-handle=6352,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=6240 /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:	133.0.3065.92

8000	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --disable-quic --string-annotations --always-read-main-dll --field-trial-handle=5612,i,14124658337064150998,1648727050267243842, 262144 --variations-seed-version --mojo-platform-channel-handle=5560 /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:	133.0.3065.92

8080	"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 --disable-quic --string-annotations --always-read-main-dll --field-trial-handle=5444,i,14124658337064150998,1648727050267243842,	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

262144 --variations-seed-version --mojo-platform-channel-handle=5424 /prefetch:8

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	LOW	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	133.0.3065.92

8096 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
Version:	10.0.19041.1 (WinBuild.160101.0800)		

Registry activity

Total events	Read events	Write events	Delete events
3 330	3 316	14	0

Modification events

(PID) Process: (2508) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** failed_count
Value: 0

(PID) Process: (2508) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** state
Value: 2

(PID) Process: (2508) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** state
Value: 1

(PID) Process: (2508) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\StabilityMetrics
Operation: write **Name:** user_experience_metrics.stability.exited_cleanly
Value: 0

(PID) Process: (2508) 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: 09FE8095179E2F00

(PID) Process: (2508) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\1835042
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {4BC60A0A-11CE-4E0A-A4C4-11FAA3A62E2A}

(PID) Process: (2508) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\1835042
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {98003764-54DA-4C6D-8AE7-8D37FA224CA0}

(PID) Process: (2508) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\1835042
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {7BBA2BD1-52CD-47F2-A2EE-6A389D7CA40D}

(PID) Process: (2508) 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: (2508) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\1835042
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {6B472210-6EB9-4471-A6A8-6BD3DB1E0E3A}

(PID) Process: (2508) 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: 1E93E195179E2F00

(PID) Process: (2508) 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: (2508) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\Profiles
Operation: write **Name:** EnhancedLinkOpeningDefault
Value: Default

(PID) Process:	(2508) msedge.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\1835042
Operation:	write	**Name:**	WindowTabManagerFileMappingId
Value:	{C38F4635-C052-4756-BD49-96E84A00CB6D}		

Files activity

Executable files	Suspicious files	Text files	Unknown types
7	194	41	0

Dropped files

PID	Process	Filename	Type
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\ClientCertificates\LOG.old~RF18e3e3.TMP **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\ClientCertificates\LOG.old **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old~RF18e3f2.TMP **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old~RF18e3f2.TMP **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old~RF18e402.TMP **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old~RF18e412.TMP **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old~RF18e3f2.TMP **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old~RF18e431.TMP **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF18e3d3.TMP **MD5:** DBBA201B22DE9AA45258E642BD5CBFDE **SHA256:** CAAA68730183AA43A172516DCCEA7FAC02370764A337B87758887BAB62272872	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Variations **MD5:** CDDDC745A8C954DC438C931889999BDB **SHA256:** 3DC9043838386F5363AC96A01477CF3163B5118B80191576A11B32CE9894314C	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\settings.dat **MD5:** EB0AECD0551E36D91C996742D6D5BA9D **SHA256:** 86A46850BEB77118A25CC1B816E93249F169ADB5794F99A66E08000CE87F7342	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Version **MD5:** BAC9FEB21F102B8ED4CD3E469213E59B **SHA256:** 84ACD485899333CBDF5AD1F68D8C31658D5ECC9EE8DDDF62098A2218687D7E77	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\268e321d-3a0e-40ff-abdf-efc378c00bf7.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** —	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old~RF18e3e3.TMP **MD5:** 2411C2A2DC2DBCFD494D338F9CA93BC5 **SHA256:** 71185D2B5D62F66F39B305C39D8CEC72CB92DEE643D989057C5D91DC73892D48	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State **MD5:** 8BE777AB08BCB6159AD05F08C356B1E3 **SHA256:** 63581D5F06F4D66864F249ADDF040DA22B6DBE05F40F03B3FCC120FEE405EF21	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old~RF18e3e3.TMP **MD5:** B936D341FF5FF88DD93C57E66FBE2F0C **SHA256:** E45649D6492C9DD7D008C538BCBC9FC04B1B5F52C8CC875D9A3D44BDB2270E62	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old~RF18e3f2.TMP **MD5:** 9A6C83893D8CEDCD338EA67101D2631C **SHA256:** 86BB2D143F5AE2E09E63AD54C1E8A2E4A1C3C5E071DD91E4E40E5D2B4996AB27	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\552c1a41-386d-40e7-808d-9dcdcf7641c9.tmp **MD5:** 8BE777AB08BCB6159AD05F08C356B1E3 **SHA256:** 63581D5F06F4D66864F249ADDF040DA22B6DBE05F40F03B3FCC120FEE405EF21	binary

2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old **MD5:** E7F9D2B31B5BB52E8E8445A8704AA2C1 **SHA256:** 699BC2075E66384530A146BDA27AEAAEB996DFAD1C0247123C04834B22AA02CB	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old **MD5:** DB2481F2EE5CCCFADDEE7C1617C3720C **SHA256:** 8E027D3744218C6DC7D25742DE58643B568F3643131E15CE2857C5EEABEE8965	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old~RF18e48f.TMP **MD5:** BA21B982B2A17BD9552C106C837A3804 **SHA256:** 1BD9D4A70ABE58BE731BE88BE75A354E279DB35B2F6E82285483DD985A274F64	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old~RF18e4cd.TMP **MD5:** 2690389F80810E7FCEE8FD3990BC3911 **SHA256:** C5ABE5B45AC2579FB674C776E13BD332D8DA862B4B323FEADA7B51D19D0F636D	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old~RF18e4cd.TMP **MD5:** 276FF7AB9AB35096D778029682AE827A **SHA256:** 50D8BD78C70C1782C59108CBBA5CD7CAC5DED458FEC05BC82B7240CC33C7907F	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old **MD5:** 7AF411DF5CEC8406E64836643DD383DD **SHA256:** 001B7E6CBDEE87E60BAA9DC20348CDA2C45E57FB7046973F92C233DD6D90A480	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old **MD5:** 3516806433E797919407F8BC4B42CE22 **SHA256:** B4B8F7CF89A689A4FCC1C28B8E5254DD1A866F113112EB3A607E7E71A61141C9	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\a313ffd1-c7ce-4922-a766-db65f7cbada6.tmp **MD5:** A1D3B67DF37296599F37D6A1E9BE4584 **SHA256:** AB74B4D26F6AAE606204BFF44F0A6D5A49A0D214288B600E08F4FCC70A18802E	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF18e412.TMP **MD5:** 8BE777AB08BCB6159AD05F08C356B1E3 **SHA256:** 63581D5F06F4D66864F249ADDF040DA22B6DBE05F40F03B3FCC120FEE405EF21	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old **MD5:** 5948AD783882CF01713F530932E52CA0 **SHA256:** 60860F7FFAAE167540F55CD87AECFD025807DDDAD57235AC886899C40AD92F5D	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old~RF18e4cd.TMP **MD5:** 4B0A62A778A5E62C1229DC4E2BF17141 **SHA256:** 2D6EFD50F51F535CA8EAB7508D653AA2C7521C842041236C8CA786DCBA705946	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old **MD5:** A1708FDAFF179284770BB93002ACC38B **SHA256:** 8A5AE9952323213E7F05F2094261875 25E13F96AEAB059B4A0AB66456B2F6D80	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old~RF18e4ec.TMP **MD5:** 063AD8ABFBFE2B143B0D161B5B35F3F9 **SHA256:** D4BB3E584947FBB2BF1EC6F84FCCAF1D8CA274526C708581CB286C2A22356530	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\load_statistics.db-wal **MD5:** A559D14B0B049083E9CFCEB76450CE51 **SHA256:** 1F558B87FFD5EFCE8E63D68F426D202787A9F3C5F81A5C752F5F46D1DCF11269	binary
1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\fcc14154-5a93-41f6-a217-3918bfaa83c5.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports~RF18e579.TMP **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old~RF18fc8b.TMP **MD5:** DF573225F3F042E12E0A93002F13BE5B **SHA256:** 331B276C7591C6467118A72DF00A8A3494A63E7806C1DE4F5A81FF5B9F1B5FC2	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5a2a7058cf8d1e56c20e6b19a7c48eb2386d141b.tbres **MD5:** 8B6C67654F52DC25D14688FEEA7540F1 **SHA256:** 4A979E1D45F45FDE3D275AFB2C1A4CF46A7BD934A3350EE8F52FBA3ED9240E16	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old **MD5:** 01D4A47B63112E1CBF4D5E1A19141D0D **SHA256:** 2CB4E04F293E7F43C98C8E413A4137FFF7ABEBC27D0EBAC81F461DF9ECF421D8	–
1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\154979b4-4c6a-409e-91b3-b54311e766ab.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\8b0d4544beb97a69dbb9583fca5575a9aba6e37d.tbres **MD5:** 5E6DDC6971C43FFF073F441AA7DE2479 **SHA256:** F00B31296AE3BF04055C7BD92954E0B1254F0C00C609F624362C3D67D668ECA1	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old **MD5:** 50DC503805C52C3FE96E78B6284DE19E **SHA256:** B3C24396647BF7020EE89C8E5CF75092ABE7495CC8AE8ADCB01ED76E5C9F8A21	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old **MD5:** 7B19E6D63EF33C7A093C696D2BEB26A8 **SHA256:** 5CFD598200C2AE61430275D26DC7C698C57B6386472166F217BA57B8498630ED	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old~RF18fc4d.TMP **MD5:** 878C04ED6E591D995681B7552CE31FEC **SHA256:** 5CC23A16B8AB26289E45A61AEA43ABF77BE0DDB058FFD78E19D6A8D712E6500C	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\Logs\sync_diagnostic.log **MD5:** D9CABDF1A9BF4AC3A3180CE5F3528991 **SHA256:** F24193EE851A24CB81B92AAA148AF88A864488DB67787F20838F480C483A22CD	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old **MD5:** 420DC4935947C93E84887B4A2365441A **SHA256:** D013CF4212CFF86F9AF45C51CDB8B9EFA5A494005420E100AEC8F9E9B9A290E4	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old~RF18fc8b.TMP **MD5:** EE6A3DF6CDA8533C21943F13B9AD19EE **SHA256:** 55528D77D8A56FBDBBC1C93C670AB38E120911850664C60873323ACEA399C7A4	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old **MD5:** 1E0526B3299DBF217A7787D88F3B7CD1 **SHA256:** 8768AC2EE3896ED0FDD8C232828EF69298FA1FD00983974B3978DFC175157AAA	text
1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports	text

		MD5: D7517139889879331980363E24189CE	SHA256: 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945
1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000259 MD5: F6FB8363C8B002F76EE1F3A0C871C218	binary SHA256: 1CF289E23EE473252ED085702BBB7007FE7A41FD2116984A523C2878FB897B9B
1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025a MD5: 61D5AB364CD351BCF53B3CF71D9A68AD	compressed SHA256: EE615A97CF83FD32C56547806E859A44D8C8E827889C64399A4E803C70A42557
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\MANIFEST-000001 MD5: 5AF87DFD673BA2115E2FCF5CFDB727AB	binary SHA256: F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps MD5: 3692B82273B09514A7212381BA0E0098	binary SHA256: A5F47979E3D9DC7C49694D8E9E4DD8E98B45470F93161940DAFF0B96BFC84A91
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps~RF18fd37.TMP MD5: 4A164D87B3F685E409A55B31861F0AE2	binary SHA256: C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\CURRENT MD5: 46295CAC801E5D4857D09837238A6394	text SHA256: 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\favorites_diagnostic.log MD5: E8E697E010932FB498CB24F9FE109B38	text SHA256: A5C5771403BEF2C216098A6A4AAB5A8CE60F2BE8B020B1EA5B002DE7C146D015
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Browser MD5: A397E5983D4A1619E36143B4D804B870	binary SHA256: 9C70F766D3B84FC2BB298EFA37CC9191F28BEC336329CC11468CFADBC3B137F4
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old~RF18fecd.TMP MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old~RF18fedd.TMP MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old~RF18fedd.TMP MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old~RF18feed.TMP MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old~RF18feed.TMP MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old~RF18feed.TMP MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\ahokoikenoafgppiblgpenaaaolecifn\LOG MD5: 34C21D30F2B638200407B773382487EE	text SHA256: F297AD47EDE77490BB34297772F512755BDC54900AE6C6944CAD07174D808941
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Rules\LOG.old~RF18fd56.TMP MD5: E30B48D8AE2479EF529F0AB65CB1F975	text SHA256: DEE4176B1D6450A9A96383F5007E77C4C7D8CD43115F5953C139926D20C9591E
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\LOG MD5: D4BEBC6F1115009D7E015DF1A08300C4	text SHA256: A5DCC832E0455A722A7E9997D28436E78B42070FBE6045EDF30EE76FCBB0A870
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\arbitration_service_config.json MD5: 56527AB03EA90AD43D662DC6F7EDCEA5	binary SHA256: F437ED4A39E990C2349F87AEB5CEB6480AFBA642B60EAA3704ADCDEF12E87757
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RF18ff0c.TMP MD5: —	— SHA256: —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old MD5: —	— SHA256: —
1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025b MD5: 03988A018185AE55F24C4A74BCCCA5B4	compressed SHA256: E16E6421B8BD76AFA5B3734D116EE58FFD63B0252480875F2CEE5B810F5FB1AC
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\75251114-468a-480c-8406-f34d9e1376a5.tmp MD5: 3692B82273B09514A7212381BA0E0098	binary SHA256: A5F47979E3D9DC7C49694D8E9E4DD8E98B45470F93161940DAFF0B96BFC84A91
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\000001.dbtmp MD5: 46295CAC801E5D4857D09837238A6394	text SHA256: 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\ahokoikenoafgppiblgpenaaaolecifn\000001.dbtmp	text

		MD5: 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\cv_debug.log	binary
		MD5: A61B46E9545D32F6C427D7A10EAB7461	**SHA256:** F1D12980D304897ECABDB769776856B18B8D7537AA748E92E709CED8C4A3BE3A
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\ahokoikenoafgppiblgpenaaaolecifn\MANIFEST-000001	binary
		MD5: 5AF87DFD673BA2115E2FCF5CFDB727AB	**SHA256:** F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Scripts\LOG.old	text
		MD5: 4467F46FAFD7B98C4FAD46C6A7A0C41A	**SHA256:** DCED1E9A36EED5A2E1F72DB8C286907D0557D54F2C0AD0E5C88E512540CE913D
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Scripts\LOG.old~RF18fd56.TMP	text
		MD5: D392F4191F0DFF78511FBDE7E3E08BF6	**SHA256:** 2AEA14504BC6FD1BD5869775B27795446DE98AED4A5C8D8D467E2F542F935A5E
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Extension Settings\ahokoikenoafgppiblgpenaaaolecifn\CURRENT	text
		MD5: 46295CAC801E5D4857D09837238A6394	**SHA256:** 0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Rules\LOG.old	—
		MD5: B6EEDEF7C3705F0AEDABF5B08F3010B5	**SHA256:** B57035BCAFF2760BC3234283F62E186F3BB43644744144770FBF9A5C45B5D299
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\000017.ldb	binary
		MD5: 659152AE3F0934F27D6E96C22FA7AF51	**SHA256:** E4B0D3ABE44B5FBA63C5954DD685B63D441CCFA992A6DE5F9D83CA9F75B1D5CC
7768	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\domains_config.json	binary
		MD5: A39A999C7D33A247283154DB645A8825	**SHA256:** 16B6E4E735848EA63B00EF42B883929E8010CAEF394EAFEACFEE02C453729A16
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\000013.log	binary
		MD5: 9C1D28D19007551398799B2F5C6D75EC	**SHA256:** 0FD996AB4C83BFA307C0ED6285B3F3088A17D21DC923819DCC8342BE6F783100
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\msedge_url_fetcher_2508_1394613867\GHBMNNJOOEKPMOECNNNILNNBDLOLHKHI_1_96_1_0.crx	binary
		MD5: D6A332CEAA785F20D7CF0EF7B9FC4790	**SHA256:** 23B8196B76670FFAC8063A91542118344BDA24D7B2FA4A4C0DD146C4EE6B31B9
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\extensions_crx_cache\ghbmnnjooekpmoecnnnilnnbdlolhkhi_1.23b8196b76670ffac8063a91542118344bda24d7b2fa4a4c0dd146c4ee6b31b9	binary
		MD5: D6A332CEAA785F20D7CF0EF7B9FC4790	**SHA256:** 23B8196B76670FFAC8063A91542118344BDA24D7B2FA4A4C0DD146C4EE6B31B9
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RF18ff1b.TMP	—
		MD5: —	**SHA256:** —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old	—
		MD5: —	**SHA256:** —
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old~RF18ff3b.TMP	—
		MD5: —	**SHA256:** —
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203\offscreendocument.html	html
		MD5: B747B5922A0BC74BBF0A9BC59DF7685F	**SHA256:** B9FA2D52A4FFABB438B56184131B893B04655B01F336066415D4FE839EFE64E7
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old	—
		MD5: —	**SHA256:** —
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ka\messages.json	binary
		MD5: 83F81D30913DC4344573D7A58BD20D85	**SHA256:** 30898BBF51BDD58DB397FF780F061E33431A38EF5CFC288B5177ECF76B399F26
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203\128.png	image
		MD5: D056CEC3B05D6A863DDFA7EE4C1C9F0C	**SHA256:** FF702CA753A7E3B75F9D9850CC9343E28E8D60F8005A2C955C8AC2105532B2C9
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203\dasherSettingSchema.json	binary
		MD5: 4EC1DF2DA46182103D2FFC3B92D20CA5	**SHA256:** 6C69CE0FE6FAB14F1990A320D704FEE362C175C00EB6C9224AA6F41108918CA6
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\pt_BR\messages.json	binary
		MD5: 8E24EC937237F48AC98B27F47B688C90	**SHA256:** A6AD5D5FB7C90736E04F898970D2CC9D423415B54B8E572F18C05D6EBAF46F68
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\it\messages.json	binary
		MD5: 88A9ACD41521D1D00B870E2DA3044A88	**SHA256:** 3377A873DB531113D79919E7A89369A79A602BAC6AE09B9864B9378DC285F345
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\lv\messages.json	binary
		MD5: 20FA89BA92628F56D36AE5BD0909CB15	**SHA256:** 80D64F03DC2CC5283FAF1354E05D3C3CB8F0CC54B3E76FDAE3AD8A09C9D5F267
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\zh_CN\messages.json	binary
		MD5: 17136B589BDA9CE7E2E5B3577B89FCB1	**SHA256:** 31EB4FFDDCCEC09F1D797D5C250B096E12022290B07A9AB0304E9751A145E815
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\no\messages.json	binary
		MD5: 66439BA3ED5BA0C702EF94793E15DE83	**SHA256:** B3ECE279943B28C8D855EC86AC1CE53BDFB6A709240D653508764493A75F7518
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\cy\messages.json	binary
		MD5: A86407C6F20818972B80B9384ACFBBED	**SHA256:** A482663292A913B02A9CDE4635C7C92270BF3C8726FD274475DC2C490019A7C9
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\be\messages.json	binary
		MD5: 68884DFDA320B85F9FC5244C2DD00568	**SHA256:** DDF16859A15F3EB3334D6241975CA3988AC3EAFC3D96452AC3A4AFD3644C8550
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\hy\messages.json	binary
		MD5: 55DE859AD778E0AA9D950EF505B29DA9	**SHA256:** 0B16E3F8BD904A767284345AE86A0A9927C47AFE89E05EA2B13AD80009BDF9E4
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\sk\messages.json	binary
		MD5: A46E08B45BE0532E461E007E894B94F4	**SHA256:** 5E886E7B616FBFF3671DAB632D1B6D8DCEEFF9004218485F1B911DCD8C9694A3

8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\bg\messages.json **MD5:** 361B516EDF253851044DAE6BAD6D9D6F **SHA256:** 22BC37B47CE8A832F39701641DC358357676E9BE187A93A4C5D4B016E29238AE	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\th\messages.json **MD5:** 0875B0BAD81161CCF2C16E13EE49AF9D **SHA256:** D299AA0C4F29C5C8248A1C51AFDB7439F4CF7BC28EE02408A598F8AAD9F70810	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\hu\messages.json **MD5:** FB8D08676AA88683F27A2759C5837529 **SHA256:** CF26310B073B0891996ECD761C6CB53F00193DEE524213A9FB34225D636EC4B7	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\am\messages.json **MD5:** 83E0E58D0752FF7C3F888E6406413B84 **SHA256:** 64E01BC292BA2EA1699576FCC445367047520EE895E290CCEE20C24C9336D8EF	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\is\messages.json **MD5:** CAEB37F451B5B5E9F5EB2E7E7F46E2D7 **SHA256:** 943E61988C859BB088F548889F0449885525DD660626A89BA67B2C94CFBFBB1B	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\es\messages.json **MD5:** 59CB3A9999DFBD19C3E3098F3B067634 **SHA256:** 02168993A23E074E0800CBB338FE279F99EF420E326BF92916FFED83C1F06533	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\te\messages.json **MD5:** 50AB4DEABAD394D13C265B8B80D9F9C3 **SHA256:** 90868A8A4A4DBF48770C14A161FAEA406EF9A453B75F4CB7A53C1B4E96A88599	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ru\messages.json **MD5:** 1CFEF8B745C04E86C62AEF09371F6489 **SHA256:** 887BC5F4575C717AE7A498A3D61E99232327170A333CFCBD9880DF1E8BCC546B	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\af\messages.json **MD5:** 7BC8FED14870159B4770D2B43B95776B **SHA256:** AA12205B108750CF9FA0978461A6D8881E4E80DA20A846D824DA4069D9C91847	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\zh_TW\messages.json **MD5:** B571E4CEFD96A2651FFB6621C4D3D1B4 **SHA256:** 16B8F7BE42B982D5AD9F638E71DA38D134394B9BAB9255F73CF514ABBFAAF146	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ml\messages.json **MD5:** CE70315E2AAEDA0999DA38CC9FE65281 **SHA256:** 907F2709D1D3C8FA26294938F4080BC477E62281C4C50A082C22DB0195CDA663	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\bn\messages.json **MD5:** B1101FAC65CE2FAA3702E70FD88957D2 **SHA256:** 3E3CEAA214D8079B02C9C941635F5D45E621236D9C3F82E06AC604F0772670E8	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RF18ff6a.TMP **MD5:** — **SHA256:** —	—
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old **MD5:** — **SHA256:** —	—
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\zh_HK\messages.json **MD5:** 524E1B2A370D0E71342D05DDE3D3E774 **SHA256:** 30F44CFAD052D73D86D12FA20CFC111563A3B2E4523B43F7D66D934BA8DACE91	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\eu\messages.json **MD5:** 29A1DA4ACB4C9D04F080BB101E204E93 **SHA256:** A41670D52423BA69C7A65E7E153E7B9994E8DD0370C584BDA0714BD61C49C578	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\km\messages.json **MD5:** B3699C20A94776A5C2F90AEF6EB0DAD9 **SHA256:** A6118F0A0DE329E07C01F53CD6FB4FED43E54C5F53DB4CD1C7F5B2B4D9FB10E6	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\sl\messages.json **MD5:** 9CDFA5371F28427F129D200338C47494 **SHA256:** 75D018CC8525605DDC591F6BFE5BDAA2EFB164934E9D5438972651F8C818D581	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\fa\messages.json **MD5:** E578E08EE604158D674982BA060396FD **SHA256:** E758273C25FBAD804FE884584E2797CAEFBBD1C2877DFD6F87AB1340CD25252E	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\fr\messages.json **MD5:** 85718FE4820C674C5305D33DFB5CBDDC **SHA256:** 6713B69B6C9E80B03E0A9D4A7D158197B0C7EC8A853C64C0AF0B1A05CE54D74C	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\kk\messages.json **MD5:** 2D94A58795F7B1E6E43C9656A147AD3C **SHA256:** 548DC6C96E31A16CE355DC55C64833B08EF3FBA8BF33149031B4A685959E3AF4	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\hr\messages.json **MD5:** EB6C5133C1FE7F9E8E4449A917D185D9 **SHA256:** 985976B776E729835E047C81D3D731A6C488A6459AA8918DBC8EC808C0BF73A1	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\en_CA\messages.json **MD5:** 558659936250E03CC14B60EBF648AA09 **SHA256:** 2445CAD863BE47BB1C15B57A4960B7B0D01864E63CDFDE6395F3B2689DC1444B	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\et\messages.json **MD5:** B18007BFC2B55D2F5839A8912110B98D **SHA256:** 7CCC7B17BFE01C3C7DD33EFF8F80D0B57FC9B175815E766C9C1C1E893725E20F	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ar\messages.json **MD5:** C825621044E4D5C504404DAE9752285C **SHA256:** 47652115CBB912907F405992FCFC64F987642158F0CB35C9D6E0D4742D833802	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\de\messages.json **MD5:** 5DAF77AE7D2B7DBEF44C5CF7E19805EE **SHA256:** 22E2828BFDBB9C340E7806894AE0442BD6C8934F85FBB964295EDAD79FD27528	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\fr_CA\messages.json **MD5:** 681422E3FCF8711AF8EEFBB75A607C8E **SHA256:** AF889C1DEB6F9248961C2F8BA4307A8206D7163616A5B7455D17CEAD00068317	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ta\messages.json **MD5:** 24626AD7B8058866033738380776F59B **SHA256:** 3FC7F56F6D6D514B32547509B39F6380FC786EFBCCA4B9859F204456CA2E7957	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\sw\messages.json **MD5:** 84EB1D6E827E40C578469EAAB778E368 **SHA256:** 2C6B42D122943DC0CA92A33074D1A607351D3BC7F9768E174617FA7011A3DE9F	binary

8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\si\messages.json **MD5:** B8A4FD612534A171A9A03C1984BB4BDD **SHA256:** 54241EBE651A8344235CC47AFD274C080ABAEBC8C3A25AFB95D8373B6A5670A2	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\mr\messages.json **MD5:** 34CE3FA84E699BCE78E026D0F0A0C705 **SHA256:** 275E7FADB93A810328E3ADEAD8754DD0A19A062D5D20A872F7471FFAB47AA7B3	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\es_419\messages.json **MD5:** 94BC2D5609F6D670E181E1FF0D041869 **SHA256:** E848603B7A73A88E3FE7BFFA20E83397F5D1E93E77BABB31473CC99E654A27B7	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\lt\messages.json **MD5:** 8047409DCC27BFCC97B3ABCE6DAB20EF **SHA256:** B42EBFE071EF0EC4B4B6553ABF3A2C36B19792C238080A6FBC19D804D1ACB61C	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\mn\messages.json **MD5:** 83E7A14B7FC60D4C66BF313C8A2BEF0B **SHA256:** 613D8751F6CC9D3FA319F4B7EA8B2BD3BED37FD077482CA825929DD7C12A69A8	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\my\messages.json **MD5:** 342335A22F1886B8BC92008597326B24 **SHA256:** 243BEFBD6B67A21433DCC97DC1A728896D3A070DC20055EB04D644E1BB955FE7	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\id\messages.json **MD5:** 3FEFE403F5F537D9A2D28AB36B2C1A94 **SHA256:** 35872A3343D4B4768FE4702A8DC18B749933E81210DB13466AD172BD2880F6EB	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\gl\messages.json **MD5:** CC31777E68B20F10A394162EE3CEE03A **SHA256:** 9890710DF0FBF1DB41BCE41FE2F62424A3BD39D755D29E829744ED3DA0C2CE1D	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\pt_PT\messages.json **MD5:** AA431EC252B4339A49D172C6B9292BA3 **SHA256:** 156FC7BA9B5728908E1A74950B97474F73D8F58933D345C8EEEA8284565C8357	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\en_US\messages.json **MD5:** 64EAEB92CB15BF128429C2354EF22977 **SHA256:** 4F70ECA8E28541855A11EC7A4E6B3BC6DD16C672FF9B596ECFB7715BB3B5898C	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\pl\messages.json **MD5:** 10BA7FE4CAB38642419BE8FEF9E78178 **SHA256:** 6538F562BD1BAA828C0EF0ADC5F7C96B4A0EB7814E6B9A2B585E4D3B92B0E61D	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\az\messages.json **MD5:** C603747B8578C1324DD262565F643E06 **SHA256:** 614470DA3C5034ACE649F1786BEAAAD2C94F4475BCC8858390B721F06FB7BF64	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ro\messages.json **MD5:** EE122CF26EBE1AD0CC733B117A89FF3B **SHA256:** 4ECEDB9C1F3DD0D0E3AEB86146561B3D7E58656CBDBED1A39B91737B52EC7F2C	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\cs\messages.json **MD5:** 48663A88DCF0EF6C9FADE9BEE4935B91 **SHA256:** 5A701D67910BA6C7CCEDC26E02FA707CC86A1BE57CD7D36290A3D268732A42C7	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\fi\messages.json **MD5:** 1D4778E02337674D7D0664B5E7DFCBBE **SHA256:** A822B0E66D04644D1CFBD2517736728438743162C3213F15D986E2DB85BD0213	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Platform Notifications\LOG.old **MD5:** BABCC8D7E939194DD25F3C6967321A83 **SHA256:** FE31E1ED8EDD4A1615B1CD0A01950054B163B3599AF0D45429DBE90CC1A54364	text
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\fil\messages.json **MD5:** F954B2E970DC96E5889499DB7392FD59 **SHA256:** 41CE6A7B18364EFECCED0419B42165D4F86C43643BBE1043014D4142CF86186A	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Platform Notifications\LOG.old~RF18ff79.TMP **MD5:** D12AC74C5D4F194A3B3EDD16725AD633 **SHA256:** A6F960B37913BE9CA153148E29692275CF2740DD7857E4F44C31D6725AF24280	text
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\hi\messages.json **MD5:** 4A9C9F947B479E5D89C38752AF3C70EA **SHA256:** 14895BF43CE9B76C0FF4F9AEF93DBE8BB6CA496894870CF0C007B189E0CEF00E	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\en\messages.json **MD5:** 558659936250E03CC14B60EBF648AA09 **SHA256:** 2445CAD863BE47BB1C15B57A4960B7B0D01864E63CDFDE6395F3B2689DC1444B	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ja\messages.json **MD5:** 113A674F2E4C66CC4D2A9C66ED77ADEA **SHA256:** C1094A1D8457E782F229910B70FC7AECE356AA779A423E869104946814660D35	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\sv\messages.json **MD5:** F008F729147F028A91E700008130DA52 **SHA256:** 5F4229D18E5606330146EE13BDF726E10C1E06CBB15368C47F1AE68ABE9CE4BA	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ca\messages.json **MD5:** FBB841A2982166239D68907361F41F61 **SHA256:** DE6D7B7C2427EC4E738407D7834B71941F69166B030355E00F325FF1391DF5A1	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\da\messages.json **MD5:** 0E451C9C8453577E513AABF630C275F2 **SHA256:** 94CDDB998C2C5AB40B6F074C359A60E6EEBAAA2D52A9649C22F4EA4C1B9936F2	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\en_GB\messages.json **MD5:** C4E77421F3361277F7E3AA3472B5EB10 **SHA256:** C7255E9B784C4B8DF7DF7B78F33A5737A9AB7382F73465351597B1DA9B3D5FE7	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\sr\messages.json **MD5:** C2026342237E7686B1932AF5B54F8110 **SHA256:** A3EB276FBD19DCE2B00DB6937578B214B9E33D67487659FE0BF21A86225ECE73	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\zu\messages.json **MD5:** 71F916A64F98B6D1B5D1F62D297FDEC1 **SHA256:** EC78DDD4CCF32B5D76EC701A20167C3FBD146D79A505E4FB0421FC1E5CF4AA63	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\kn\messages.json **MD5:** F55CE2E64A06806B43816AB17D8EE623 **SHA256:** 5FA00C465C1C5EED4BEA860CEB78DA9419EA115347BA543DDB0076E5C188FEED	binary
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\iw\messages.json	binary

		MD5: 26B1533C0852EE4661EC1A27BD87D6BF **SHA256:** BBB81C32F482BA3216C9B1189C70CEF39CA8C2181AF3538FFA07B4C6AD52F06A	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ko\messages.json	binary
		MD5: E71A91FE65DD32CAC3925CE639441675 **SHA256:** 57F81A5FCBD1FEFD6EC3CDD525A85B707B4EEAD532C1B3092DAAFD88EE9268EC	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\lo\messages.json	binary
		MD5: E20D6C27840B406555E2F5091B118FC5 **SHA256:** 89082FB05229826BC222F5D22C158235F025F0E6DF67FF135A18BD899E13BB8F	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\tr\messages.json	binary
		MD5: 3104BCD0D4AD6B47FE36F36C1B5AA333 **SHA256:** AC2894CEA6332450095A7F8FC9B97550DA87E4B4B6E6FB95DF1A1F49F25E0E35	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\pa\messages.json	binary
		MD5: 97F769F51B83D35C260D1F8CFD7990AF **SHA256:** BBD37D41B7DE6F93948FA2437A7699D4C30A3C39E736179702F212CB36A3133C	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ur\messages.json	binary
		MD5: F6E8FCA4FD1A7AF320D4D30D6055FA6D **SHA256:** 504549057A6A182A404C36112D2450864A6CB4574CD0E8F435CA556FAC52AB0A	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\nl\messages.json	binary
		MD5: D448E11801349AB5704DF8446FE3FA4C **SHA256:** E98C5CFE277A338A938E7277DEEC132F5EA82A53EBDB65FF10E8A2FF548AC198	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\uk\messages.json	binary
		MD5: AE938164F7AC0E7C7F120742DE2BEB1E **SHA256:** 08978A1425DEC304483BBB7DD0E55A7D850C4561ABD41BAC1BE5D93D70465174	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203\manifest.json	binary
		MD5: 4EA02D707001E4A23EBCA21664B5E707 **SHA256:** A534811F18737107D8FE30C207C49E8F6C746D552EB2AA1C6C1490E20554E6BA	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ne\messages.json	binary
		MD5: 065EB4DE2319A4094F7C1C381AC753A0 **SHA256:** 160E1CD593C901C7291EA4ECBA735191D793DDFD7E9646A0560498627F61DA6F	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_metadata\verified_contents.json	text
		MD5: 3AE58BDDFAF550122CA2EEEDC8C2B2D8 **SHA256:** A4A3C5200D0CA61100175311BFC8FFD07F61CBA2F8DDE064409816C505AEFF02	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\4bf44bc9-ae03-4772-b421-2d5848bbdf5c.tmp	binary
		MD5: 5058F1AF8388633F609CADB75A75DC9D **SHA256:** —	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL\128.png	image
		MD5: 35696ABA596D5B8619A558DD05B4AD40 **SHA256:** 75DA533888189D13FC340D40637B9FC07A3F732E3FCF33EC300F4C7268790A62	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\ms\messages.json	binary
		MD5: DB4D49231C88C11E8D8C3D71A9B7D3D4 **SHA256:** 9B32C491D0BFEBDCA1455F73C3C6F71796D433A39818C06C353DA588DE650F81	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\vi\messages.json	binary
		MD5: 1E54AFBACCA335BE3A050920DDFBE863 **SHA256:** F1DA95E1D58E933050CD8A4FEA12F3D1B9A2759479FFDB74FDC1CFBF89568327	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\gu\messages.json	binary
		MD5: 86DE754C2D6B550048C9D914E55B5FF0 **SHA256:** CC3E9077FCC9BD0DFC5DD3924C6C48B8345F32CEE24FCCC508C279F45B2ABE61	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203\page_embed_script.js	binary
		MD5: D96EF6F77173A1352A55BDAD24C7274F **SHA256:** F647416D0A90C6CB07A6842DA7A5AF15AEE2659A734D7578EBB6B99DA64A7F1E	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203\service_worker_bin_prod.js	binary
		MD5: 221AC49325F64B521E99BFFE2B9C3151 **SHA256:** BB7CD8337156A951052A5C2B1FCB3FEA7DCCB2926CC3089669FB900A3B13C85D	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203\offscreendocument_main.js	binary
		MD5: A8C65709CFA5F4445855203BCE9E5927 **SHA256:** D63153DE6398ADB68AE305B509EC88DB422295CA19AB38D6F4ACD0E38B4C8366	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\bn\messages.json	binary
		MD5: 651375C6AF22E2BCD228347A45E3C2C9 **SHA256:** 1DBF38E425C5C7FC39E8077A837DF0443692463BA1FBE94E288AB5A93242C46E	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ca\messages.json	binary
		MD5: D177261FFE5F8AB4B3796D26835F8331 **SHA256:** D6E65238187A430FF29D4C10CF1C46B3F0FA4B91A5900A17C5DFD16E67FFC9BD	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\am\messages.json	binary
		MD5: 9721EBCE89EC51EB2BAEB4159E2E4D8C **SHA256:** 3D0361A85ADFCD35D0DE74135723A75B646965E775188F7DCDD35E3E42DB788E	
8000	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203_locales\el\messages.json	binary
		MD5: 32886978EF4B5231F921EB54E683EB10 **SHA256:** 728D8CBD71263680A4E41399DB65B3F2B8175D50CA630AFD30643CED9FFE831F	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping2508_868422203\manifest.fingerprint	text
		MD5: 625D1CF5FB759445101D2B987C36E031 **SHA256:** 377A421A710752D36B9282C5AC41DF845A9958C4DA5F5ABDDB55E562AFDECCE8	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\bg\messages.json	binary
		MD5: 2E6423F38E148AC5A5A041B1D5989CC0 **SHA256:** AC4A8B5B7C0B0DD1C07910F30DCFBDF1BCB701CFCFD182B6153FD3911D566C0E	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\af\messages.json	binary
		MD5: 12403EBCCE3AE8287A9E823C0256D205 **SHA256:** B40BDE5B612CFFF936370B32FB0C58CC205FC89937729504C6C0B527B60E2CBA	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\el\messages.json	binary
		MD5: 9ABA4337C670C6349BA38FDDC27C2106 **SHA256:** 37CA6AB271D6E7C9B00B846FDB969811C9CE7864A85B5714027050795EA24F00	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\en\messages.json	binary
		MD5: 07FFBE5F24CA348723FF8C6C488ABFB8 **SHA256:** 6895648577286002F1DC9C3366F558484EB7020D52BBF64A296406E61D09599C	
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\az\messages.json	binary
		MD5: 9A798FD298008074E59ECC253E2F2933 **SHA256:** 628145F4281FA825D75F1E332998904466ABD050E8B0DC8BB9B6A20488D78A66	

2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ar\messages.json	binary
		MD5: 3EC93EA8F8422FDA079F8E5B3F386A73	**SHA256:** ABD0919121956AB535E6A235DE67764F46CFC944071FCF2302148F5FB0E8C65A
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\de\messages.json	binary
		MD5: D116453277CC860D196887CEC6432FFE	**SHA256:** 36AC525FA6E28F18572D71D75293970E0E1EAD68F358C20DA4FDC643EEA2C1C5
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\en_CA\messages.json	binary
		MD5: 07FFBE5F24CA348723FF8C6C488ABFB8	**SHA256:** 6895648577286002F1DC9C3366F558484EB7020D52BBF64A296406E61D09599C
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\en_GB\messages.json	binary
		MD5: 3734D498FB377CF5E4E2508B8131C0FA	**SHA256:** AB5CDA04013DCE0195E80AF714FBF3A67675283768FFD062CF3CF16EDB49F5D4
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\en_US\messages.json	binary
		MD5: 578215FBB8C12CB7E6CD73FBD16EC994	**SHA256:** 102B586B197EA7D6EDFEB874B97F95B05D229EA6A92780EA8544C4FF1E6BC5B1
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\cs\messages.json	binary
		MD5: CCB00C63E4814F7C46B06E4A142F2DE9	**SHA256:** 21AE66CE537095408D21670585AD12599B0F575FF2CB3EE34E3A48F8CC71CFAB
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\da\messages.json	binary
		MD5: B922F7FD0E8CCAC31B411FC26542C5BA	**SHA256:** 48847D57C75AF51A44CBF8F7EF1A4496C2007E58ED56D340724FDA1604FF9195
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\es\messages.json	binary
		MD5: F61916A206AC0E971CDCB63B29E580E3	**SHA256:** 2008F4FAAB71AB8C76A5D8811AD40102C380B6B929CE0BCE9C378A7CADFC05EB
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\fa\messages.json	binary
		MD5: 097F3BA8DE41A0AAF436C783DCFE7EF3	**SHA256:** 7C4C09D19AC4DA30CC0F7F521825F44C4DFBC19482A127FBFB2B74B3468F48F1
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\fil\messages.json	binary
		MD5: FCEA43D62605860FFF41BE26BAD80169	**SHA256:** F51EEB7AAF5F2103C1043D520E5A4DE0FA75E4DC375E23A2C2C4AFD4D9293A72
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\fr_CA\messages.json	binary
		MD5: 6CAC04BDCC09034981B4AB567B00C296	**SHA256:** 4CAA46656ECC46A420AA98D3307731E84F5AC1A89111D2E808A228C436D83834
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\es_419\messages.json	binary
		MD5: 535331F8FB98894877811B14994FEA9D	**SHA256:** 90A560FF82605DB7EDA26C90331650FF9E42C0B596CEDB79B23598DEC1B4988F
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\fr\messages.json	binary
		MD5: A58C0EEBD5DC6BB5D91DAF923BD3A2AA	**SHA256:** 0518287950A8B010FFC8D52554EB82E5D93B6C3571823B7CECA898906C11ABCC
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\fi\messages.json	binary
		MD5: B38CBD6C2C5BFAA6EE252D573A0B12A1	**SHA256:** 2D752A5DBE80E34EA9A18C958B4C754F3BC10D63279484E4DF5880B8FD1894D2
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\et\messages.json	binary
		MD5: 64204786E7A7C1ED9C241F1C59B81007	**SHA256:** CC31B877238DA6C1D51D9A6155FDE565727A1956572F466C387B7E41C4923A29
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\hu\messages.json	binary
		MD5: 8930A51E3ACE3DD897C9E61A2AEA1D02	**SHA256:** 958C0F664FCA20855FA84293566B2DDB7F297185619143457D6479E6AC81D240
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\gl\messages.json	binary
		MD5: 6BAAFEE2F718BEFBC7CD58A04CCC6C92	**SHA256:** 0CF098DFE5BBB46FC0132B3CF0C54B06B4D2C8390D847EE2A65D20F9B7480F4C
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\gu\messages.json	binary
		MD5: BC7E1D09028B085B74CB4E04D8A90814	**SHA256:** FE8218DF25DB54E633927C4A1640B1A41B8E6CB3360FA386B5382F833B0B237C
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\hi\messages.json	binary
		MD5: 98A7FC3E2E05AFFFC1CFE4A029F47476	**SHA256:** D2D1AFA224CDA388FF1DC8FAC24CDA228D7CE09DE5D375947D7207FA4A6C4F8D
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\hr\messages.json	binary
		MD5: 25CDFF9D60C5FC4740A48EF9804BF5C7	**SHA256:** 73E6E246CEEAB9875625CD4889FBF931F93B7B9DEAA11288AE1A0F8A6E311E76
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\kn\messages.json	binary
		MD5: 38BE0974108FC1CC30F13D8230EE5C40	**SHA256:** 30078EF35A76E02A400F03B3698708A0145D9B57241CC4009E010696895CF3A1
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ko\messages.json	binary
		MD5: F3E59EEEB007144EA26306C20E04C292	**SHA256:** C52D9B955D229373725A6E713334BBB31EA72EFA9B5CF4FBD76A566417B12CAC
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\lt\messages.json	binary
		MD5: 970544AB4622701FFDF66DC556847652	**SHA256:** 5DFCBD4DFEAEC3ABE973A78277D3BD02CD77AE635D5C8CD1F816446C61808F59
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\id\messages.json	binary
		MD5: 34D6EE258AF9429465AE6A078C2FB1F5	**SHA256:** E3C86DDD2EFEBE88EED8484765A9868202546149753E03A61EB7C28FD62CFCA1
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\it\messages.json	binary
		MD5: 0D82B734EF045D5FE7AA680B6A12E711	**SHA256:** F41862665B13C0B4C4F562EF1743684CCE29D4BCF7FE3EA494208DF253E33885
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ja\messages.json	binary
		MD5: 15EC1963FC113D4AD6E7E59AE5DE7C0A	**SHA256:** 34AC08F3C4F2D42962A3395508818B48CA323D22F498738CC9F09E78CB197D73
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\mr\messages.json	binary
		MD5: 3B98C4ED8874A160C3789FEAD5553CFA	**SHA256:** ADEB082A9C754DFD5A9D47340A3DDCC19BF9C7EFA6E629A2F1796305F1C9A66F
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ms\messages.json	binary
		MD5: 7D273824B1E22426C033FF5D8D7162B7	**SHA256:** 2824CF97513DC3ECC261F378BFD595AE95A5997E9D1C63F5731A58B1F8CD54F9
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\lv\messages.json	binary

		MD5: A568A58817375590007D1B8ABCAEBF82	SHA256: 0621DE9161748F45D53052ED8A430962139D7F19074C7FFE7223ECB06B0B87DB
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ml\messages.json	binary
		MD5: 4717EFE4651F94EFF6ACB6653E868D1A	SHA256: 22CA9415E294D9C3EC3384B9D08CDAF5164AF73B4E4C251559E09E529C843EA6
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ne\messages.json	binary
		MD5: B1083DA5EC718D1F2F093BD3D1FB4F37	SHA256: E6ED0A023EF31705CCCBAF1E07F2B4B2279059296B5CA973D2070417BA16F790
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\nl\messages.json	binary
		MD5: 32DF72F14BE59A9BC9777113A8B21DE6	SHA256: F3FE1FFCB182183B76E1B46C4463168C746A38E461FD25CA91FF2A40846F1D61
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\no\messages.json	binary
		MD5: A1744B0F53CCF889955B95108367F9C8	SHA256: 21CEFF02B45A4BFD60D144879DFA9F427949A027DD49A3EB0E9E345BD0B7C9A8
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\pl\messages.json	binary
		MD5: B8D55E4E3B9619784AECA61BA15C9C0F	SHA256: E00FF20437599A5C184CA0C79546CB6500171A95E5F24B9B5535E89A89D3EC3D
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\pt_BR\messages.json	binary
		MD5: 608551F7026E6BA8C0CF85D9AC11F8E3	SHA256: A73EEA087164620FA2260D3910D3FBE302ED85F454EDB1493A4F287D42FC882F
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\pt_PT\messages.json	binary
		MD5: 0963F2F3641A62A78B02825F6FA3941C	SHA256: E93B8E7FB86D2F7DFAE57416BB1FB6EE0EEA25629B972A5922940F0023C85F90
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ro\messages.json	binary
		MD5: BED8332AB788098D276B448EC2B33351	SHA256: 085787999D78FADFF9600C9DC5E3FF4FB4EB9BE06D6BB19DF2EEF8C284BE7B20
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\sk\messages.json	binary
		MD5: 8E55817BF7A87052F11FE554A61C52D5	SHA256: 903060EC9E76040B46DEB47BBB041D0B28A6816CB9B892D7342FC7DC6782F87C
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ru\messages.json	binary
		MD5: 1CA9A6BD3D62B1ABEC854FF1864E10B9	SHA256: C0A776448A258EFD47065BF3F4B45260D1B4CB431D57ECC97995E122249081F6
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\sl\messages.json	binary
		MD5: BFAEFEFF32813DF91C56B71B79EC2AF4	SHA256: AAB9CF9098294A46DC0F2FA468AFFF7CA7C323A1A0EFA70C9DB1E3A4DA05D1D4
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\sr\messages.json	binary
		MD5: 7F5F8933D2D078618496C67526A2B066	SHA256: 4E8B69E864F57CDDD4DC4E4FAF2C28D496874D06016BC22E8D39E0CB69552769
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\sv\messages.json	binary
		MD5: 90D8FB448CE9C0B9BA3D07FB8DE6D7EE	SHA256: 64B1E422B346AB77C5D1C77142685B3FF7661D498767D104B0C24CB36D0EB859
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\sw\messages.json	binary
		MD5: D0579209686889E079D87C23817EDDD5	SHA256: 0D20680B74AF10EF8C754FCDE259124A438DCE3848305B0CAF994D98E787D263
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\te\messages.json	binary
		MD5: 385E65EF723F1C4018EEE6E4E56BC03F	SHA256: 026C164BAE27DBB36A564888A796AA3F188AAD9E0C37176D48910395CF772CEA
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ta\messages.json	binary
		MD5: DCC0D1725AEAEAAF1690EF8053529601	SHA256: 6282BF9DF12AD453858B0B531C8999D5FD6251EB855234546A1B30858462231A
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\th\messages.json	binary
		MD5: 64077E3D186E585A8BEA86FF415AA19D	SHA256: D147631B2334A25B8AA4519E4A30FB3A1A85B6A0396BC688C68DC124EC387D58
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\tr\messages.json	binary
		MD5: 76B59AAACC7B469792694CF3855D3F4C	SHA256: B9066A162BEE00FD50DC48C71B32B69DFFA362A01F84B45698B017A624F46824
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\uk\messages.json	binary
		MD5: 970963C25C2CEF16BB6F60952E103105	SHA256: 9FA26FF09F6ACDE2457ED366C0C4124B6CAC1435D0C4FD8A870A0C090417DA19
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\ur\messages.json	binary
		MD5: 8B4DF6A9281333341C939C244DDB7648	SHA256: 5DA836224D0F3A96F1C5EB5063061AAD837CA9FC6FED15D19C66DA25CF56F8AC
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\vi\messages.json	binary
		MD5: 773A3B9E708D052D6CBAA6D55C8A5438	SHA256: 597C5F32BC999746BC5C2ED1E5115C523B7EB1D33F81B042203E1C1DF4BBCAFE
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\zh_CN\messages.json	binary
		MD5: DE9899623560D8A6F389CB0726ABFA7C	SHA256: C047235C983D3DCF835D4ECC1C9270C6262A09A5ACADF093D87E709C0A23CAE7
2508	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir2508_958063545\CRX_INSTALL_locales\zh_TW\messages.json	binary
		MD5: 0E60627ACFD18F44D4DF469D8DCE6D30	SHA256: F94C6DDEDF067642A1AF18D629778EC65E02B6097A8532B7E794502747AEB008
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\bac75876-fb45-483f-952b-23d9ade2419a.tmp	binary
		MD5: 3CDEB3D5E39D216F8307946B1FE49B85	SHA256: 39ED54E12E51E3B8B6B595F4512505EB1CF8589605115F4B1480582C26A78929
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\4583aa49-4a59-45e3-9781-6d64afd9116b.tmp	binary
		MD5: DDD492DF36AA406EDE2A76E2064007D2	SHA256: 470108EF9C46D3F98D0CA5ACBA287B75D02ED41768A28BD59A48E391E6EA0360
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF190b12.TMP	binary
		MD5: A1D3B67DF37296599F37D6A1E9BE4584	SHA256: AB74B4D26F6AAE606204BFF44F0A6D5A49A0D214288B600E08F4FCC70A18802E
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF190b12.TMP	binary
		MD5: 5D29912EF62E9B787E671EFD59A7FB0F	SHA256: 1A92FAC7708A1495242F7801EC82FA6A2ADBA89EFAECC9DCE17F690E84DC62C5
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences	binary
		MD5: DDD492DF36AA406EDE2A76E2064007D2	SHA256: 470108EF9C46D3F98D0CA5ACBA287B75D02ED41768A28BD59A48E391E6EA0360

1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\cb16a61d-7f1c-436a-ba92-8aa461b6575e.tmp **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries~RF190bed.TMP **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
1944	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\0ed6c038-09e8-442e-81d5-9c2e33df320d.tmp **MD5:** DD21339BF1088AFB2BB0F18F254F10CE **SHA256:** EACEABA8ECBFC21FCAEFAB8B140FD50313C7E4684A5DBDC834425866119BD265	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Secure Preferences~RF19234d.TMP **MD5:** FD0590F7515930B5D8BD648556BB62A9 **SHA256:** 742FC37B1E5D054A7CF3B9A8304A88F003EC442405B0D688E5ACAF74AE8F0066	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Secure Preferences **MD5:** DD21339BF1088AFB2BB0F18F254F10CE **SHA256:** EACEABA8ECBFC21FCAEFAB8B140FD50313C7E4684A5DBDC834425866119BD265	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF193212.TMP **MD5:** DDD492DF36AA406EDE2A76E2064007D2 **SHA256:** 470108EF9C46D3F98D0CA5ACBA287B75D02ED41768A28BD59A48E391E6EA0360	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\642de7a7-8aa3-4ab2-9e99-a878dcb80807.tmp **MD5:** B0FD22D6B14D60B5EA5EFB7132A49781 **SHA256:** 6BF9B301E74623B5BD0EB0F8C2D44B1F2A6E51D932BED2CDD9020BC01FC99355	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\f31c175a-349e-4cfb-aace-d82058afc815.tmp **MD5:** 912BA9A2A390EA874BAF7616A943C476 **SHA256:** DF193EC993CCB3C1CA7C707B0223FBB2D01C8C3C7CA62D81CFE796EFE6830AF1	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF19336a.TMP **MD5:** 3CDEB3D5E39D216F8307946B1FE49B85 **SHA256:** 39ED54E12E51E3B8B6B595F4512505EB1CF8589605115F4B1480582C26A78929	binary
7768	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\000003.log **MD5:** 69EE88F5C6754E98FB823532CADF3EE0 **SHA256:** 109EE23D7CB09E6C5E32E4B72A015D86E8E321A234C0C6D402E29333291657B6	binary
7768	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG **MD5:** 34EA5E1F45C1C35C2BB8B22862B17E33 **SHA256:** 057F9457EE85F57B4BF8F0D79A7EB00937202B0F6AA2EB59A98FC860C3EF8B05	text
7760	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\000013.log **MD5:** 44C64889158FA78E48C6B56054372C67 **SHA256:** BA38B5BBA46B384E3D35AC6A0FC9C309AE864E8E0C2A2399AD11C8AA0DAB0F73	binary
7760	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG **MD5:** DC1D0786E0F85F3699AEF6C7E4834BEA **SHA256:** 8DDE88B2F5CD2FA904AA7411EB724DEA0808B96E43BABAF004534447B6C36390	text
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\94a2e61b-5e7e-4584-9ac1-ea1846660184.tmp **MD5:** 912BA9A2A390EA874BAF7616A943C476 **SHA256:** DF193EC993CCB3C1CA7C707B0223FBB2D01C8C3C7CA62D81CFE796EFE6830AF1	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\ade835c4-063c-43a1-a04b-d125e56cd41b.tmp **MD5:** E054D0CBDD65DD2400E9DB9FD3B3C4CC **SHA256:** 4592A818F5720BC23AD6667BC25F27452F090A28C93751001CE5D48CD1F10E61	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF198032.TMP **MD5:** 912BA9A2A390EA874BAF7616A943C476 **SHA256:** DF193EC993CCB3C1CA7C707B0223FBB2D01C8C3C7CA62D81CFE796EFE6830AF1	binary
2508	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF198052.TMP **MD5:** B0FD22D6B14D60B5EA5EFB7132A49781 **SHA256:** 6BF9B301E74623B5BD0EB0F8C2D44B1F2A6E51D932BED2CDD9020BC01FC99355	binary

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
13	45	48	10

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1944	msedge.exe	GET	200	150.171.28.11:80	http://edge.microsoft.com/browsernetworktime/time/1/current?cup2key=2:OClv4x5l-oMWofJY_1xCz-hfxXeX2l95XVS72rRVCM0&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	unknown	–	–	whitelisted
2760	svchost.exe	GET	200	162.159.142.9:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
1944	msedge.exe	GET	200	176.100.39.60:80	http://zntsfboczi.rd.klockars.com/4HLNCy3713Lzgc273iqwcbcyxtq146KUKCHPYUBZWBTFM394829SAJX1570z1	unknown	–	–	–
1268	svchost.exe	GET	200	23.216.77.28:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
1268	svchost.exe	GET	200	23.3.109.244:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	whitelisted
3460	SIHClient.exe	GET	200	2.23.190.84:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted

3460	SIHClient.exe	GET	200	2.23.190.84:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	whitelisted
3460	SIHClient.exe	GET	200	2.23.190.84:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
3460	SIHClient.exe	GET	200	23.55.110.193:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut_2010-06-23.crl	unknown	—	—	whitelisted
3460	SIHClient.exe	GET	200	2.23.190.84:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Time-Stamp%20PCA%202010(1).crl	unknown	—	—	whitelisted
3460	SIHClient.exe	GET	200	2.23.190.84:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.2.crl	unknown	—	—	whitelisted
3460	SIHClient.exe	GET	200	2.23.190.84:80	http://www.microsoft.com/pkiops/crl/Microsoft%20Update%20Signing%20CA%202.1.crl	unknown	—	—	whitelisted
3460	SIHClient.exe	GET	200	2.23.190.84:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Signing%20CA%202.1.crl	unknown	—	—	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1268	svchost.exe	4.231.128.59:443	—	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:137	—	—	—	whitelisted
5944	MoUsoCoreWorker.exe	4.231.128.59:443	—	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
6292	RUXIMICS.exe	4.231.128.59:443	—	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
1944	msedge.exe	150.171.22.17:443	config.edge.skype.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1944	msedge.exe	150.171.28.11:80	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1944	msedge.exe	52.102.113.35:443	na01.safelinks.protection.outlook.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1944	msedge.exe	150.171.28.11:443	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1944	msedge.exe	2.16.241.224:443	copilot.microsoft.com	Akamai International B.V.	DE	whitelisted
2760	svchost.exe	40.126.32.136:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
2760	svchost.exe	162.159.142.9:80	ocsp.digicert.com	CLOUDFLARENET	—	whitelisted
1944	msedge.exe	176.100.39.60:443	zntsfboczi.rd.klockars.com	intercolo GmbH	DE	unknown
1944	msedge.exe	176.100.39.60:80	zntsfboczi.rd.klockars.com	intercolo GmbH	DE	unknown
1944	msedge.exe	23.11.206.107:443	www.bing.com	Akamai International B.V.	DE	whitelisted
1944	msedge.exe	188.114.97.3:443	www.herbolx.com	CLOUDFLARENET	NL	whitelisted
1268	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1268	svchost.exe	23.216.77.28:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
1268	svchost.exe	23.3.109.244:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
1944	msedge.exe	142.250.185.195:443	update.googleapis.com	GOOGLE	US	whitelisted
1944	msedge.exe	216.58.212.161:443	clients2.googleusercontent.com	GOOGLE	US	whitelisted
1944	msedge.exe	150.171.27.11:443	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1944	msedge.exe	13.107.246.45:443	edgeassetservice.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
2508	msedge.exe	224.0.0.251:5353	—	—	—	whitelisted
1944	msedge.exe	142.250.181.234:443	www.googleapis.com	GOOGLE	US	whitelisted
5944	MoUsoCoreWorker.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5944	MoUsoCoreWorker.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1268	svchost.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
3460	SIHClient.exe	74.178.76.128:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
3460	SIHClient.exe	2.23.190.84:80	www.microsoft.com	AKAMAI-AS	BR	whitelisted
3460	SIHClient.exe	23.55.110.193:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
3460	SIHClient.exe	40.69.42.241:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
1944	msedge.exe	13.107.246.44:443	edge-consumer-static.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

4040	slui.exe	4.154.209.85:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

DNS requests

Domain	IP	Reputation
google.com	142.250.185.110	whitelisted
edge.microsoft.com	150.171.28.11 150.171.27.11	whitelisted
config.edge.skype.com	150.171.22.17	whitelisted
na01.safelinks.protection.outlook.com	52.102.113.35 52.102.113.53 52.102.113.28 52.102.113.60 52.102.113.21 52.102.113.32 52.102.113.27 52.102.113.36	whitelisted
copilot.microsoft.com	2.16.241.224 2.16.241.220	whitelisted
login.live.com	40.126.32.136 40.126.32.138 40.126.32.72 40.126.32.68 20.190.160.3 20.190.160.67 20.190.160.64 20.190.160.17	whitelisted
ocsp.digicert.com	162.159.142.9 172.66.2.5	whitelisted
zntsfboczi.rd.klockars.com	176.100.39.60	unknown
www.bing.com	23.11.206.107 23.11.206.98	whitelisted
www.herbolx.com	188.114.97.3 188.114.96.3	unknown
settings-win.data.microsoft.com	20.73.194.208 51.124.78.146 51.104.136.2	whitelisted
crl.microsoft.com	23.216.77.28 23.216.77.6 23.55.110.193 23.55.110.211	whitelisted
www.microsoft.com	23.3.109.244 2.23.190.84	whitelisted
update.googleapis.com	142.250.185.195	whitelisted
clients2.googleusercontent.com	216.58.212.161	whitelisted
edgeassetservice.azureedge.net	13.107.246.45	whitelisted
www.googleapis.com	142.250.181.234 172.217.16.202 142.250.186.106 216.58.206.42 142.250.185.138 142.250.186.138 142.250.185.74 142.250.186.170 142.250.185.170 142.250.185.202 216.58.212.138 142.250.186.42 142.250.185.106 216.58.206.74 142.250.186.74 142.250.185.234	whitelisted
slscr.update.microsoft.com	74.178.76.128	whitelisted
fe3cr.delivery.mp.microsoft.com	40.69.42.241	whitelisted
edge-consumer-static.azureedge.net	13.107.246.44 13.107.213.44	whitelisted
self.events.data.microsoft.com	20.189.173.7	whitelisted

activation-v2.sls.microsoft.com	4.154.209.85	whitelisted

Threats

PID	Process	Class	Message
—	—	Potentially Bad Traffic	ET DYN_DNS DYNAMIC_DNS Query to a *.klockars .com Domain
—	—	Potentially Bad Traffic	ET DYN_DNS DYNAMIC_DNS Query to a *.klockars .com Domain
—	—	Potentially Bad Traffic	ET DYN_DNS DYNAMIC_DNS Query to a *.klockars .com Domain
—	—	Potentially Bad Traffic	ET DYN_DNS DYNAMIC_DNS Query to a *.klockars .com Domain
—	—	Potentially Bad Traffic	ET DYN_DNS DYNAMIC_DNS Query to a *.klockars .com Domain
—	—	Potentially Bad Traffic	ET DYN_DNS DYNAMIC_DNS Query to a *.klockars .com Domain
—	—	Potentially Bad Traffic	ET DYN_DNS DYNAMIC_DNS HTTP Request to a *.klockars .com Domain
—	—	Possible Social Engineering Attempted	REDIRECT [ANY.RUN] Fake Market FoxWhoops Evil Redirect
—	—	Unknown Traffic	ET USER_AGENTS Microsoft Dr Watson User-Agent (MSDW)
—	—	Potentially Bad Traffic	ET INFO Possible Chrome Plugin install

Debug output strings

No debug info