ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	butterflyondesktop.exe
Full analysis:	https://app.any.run/tasks/3a448a27-86c0-479c-ab0b-d78c44d5fd77
Verdict:	Malicious activity
Analysis date:	March 05, 2025 at 21:50:03
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	auto generic inno installer delphi
Indicators:	
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, 8 sections
MD5:	1535AA21451192109B86BE9BCC7C4345
SHA1:	1AF211C686C4D4BF0239ED6620358A19691CF88C
SHA256:	4641AF6A0071E11E13AD3B1CD950E01300542C2B9EFB6AE92FFECEDDE974A4A6
SSDEEP:	49152:5aA7f7tlVmdqK23H2bpHI4Qs5ABV9WRHZRsgI82lcHGAaKLinXBgJ:Q+VMkX224QsWBq5SfARGRgJ

Software environment set and analysis options

Launch configuration

Task duration:	150 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	on	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

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

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

- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)
- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)

Behavior activities

MALICIOUS

GENERIC has been found (auto)
- butterflyondesktop.exe (PID: 2392)

Changes the autorun value in the registry
- butterflyondesktop.tmp (PID: 1228)

SUSPICIOUS

Reads security settings of Internet Explorer
- butterflyondesktop.tmp (PID: 5544)
- butterflyondesktop.tmp (PID: 1228)

Executable content was dropped or overwritten
- butterflyondesktop.exe (PID: 2392)
- butterflyondesktop.exe (PID: 1164)
- butterflyondesktop.tmp (PID: 1228)

Process drops legitimate windows executable
- butterflyondesktop.tmp (PID: 1228)

Reads the Windows owner or organization settings
- butterflyondesktop.tmp (PID: 1228)

There is functionality for taking screenshot (YARA)
- ButterflyOnDesktop.exe (PID: 5680)

INFO

Checks supported languages
- butterflyondesktop.tmp (PID: 5544)
- butterflyondesktop.exe (PID: 2392)
- butterflyondesktop.exe (PID: 1164)
- butterflyondesktop.tmp (PID: 1228)
- identity_helper.exe (PID: 7844)
- ButterflyOnDesktop.exe (PID: 5680)

Create files in a temporary directory
- butterflyondesktop.exe (PID: 2392)
- butterflyondesktop.exe (PID: 1164)
- butterflyondesktop.tmp (PID: 1228)

Reads the computer name
- butterflyondesktop.tmp (PID: 5544)
- butterflyondesktop.tmp (PID: 1228)
- identity_helper.exe (PID: 7844)
- ButterflyOnDesktop.exe (PID: 5680)

Process checks computer location settings
- butterflyondesktop.tmp (PID: 5544)

Compiled with Borland Delphi (YARA)
- butterflyondesktop.tmp (PID: 5544)
- slui.exe (PID: 1348)
- butterflyondesktop.tmp (PID: 1228)
- ButterflyOnDesktop.exe (PID: 5680)

Detects InnoSetup installer (YARA)
- butterflyondesktop.exe (PID: 1164)
- butterflyondesktop.tmp (PID: 5544)
- butterflyondesktop.exe (PID: 2392)
- butterflyondesktop.tmp (PID: 1228)

Creates files in the program directory
- butterflyondesktop.tmp (PID: 1228)

Creates a software uninstall entry
- butterflyondesktop.tmp (PID: 1228)

The sample compiled with english language support
- butterflyondesktop.tmp (PID: 1228)

Reads Environment values
- identity_helper.exe (PID: 7844)

Manual execution by a user
- msedge.exe (PID: 1328)

Application launched itself
- msedge.exe (PID: 6040)
- msedge.exe (PID: 1328)

Reads the software policy settings
- slui.exe (PID: 1348)

Checks proxy server information
- slui.exe (PID: 1348)

Malware configuration

No Malware configuration.

Static information

TRiD

.exe | Inno Setup installer (77.7)
.exe | Win32 Executable Delphi generic (10)
.dll | Win32 Dynamic Link Library (generic) (4.6)
.exe | Win32 Executable (generic) (3.1)

EXIF

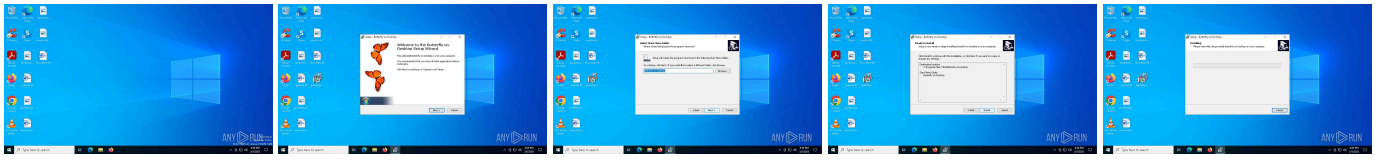
EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	1992:06:19 22:22:17+00:00
ImageFileCharacteristics:	No relocs, Executable, No line numbers, No symbols, Bytes r eversed lo, 32-bit, Bytes reversed hi

.exe | Win16/32 Executable Delphi generic (1.4)

PEType:	PE32
LinkerVersion:	2.25
CodeSize:	37888
InitializedDataSize:	17920
UninitializedDataSize:	-
EntryPoint:	0x9c40
OSVersion:	1
ImageVersion:	6
SubsystemVersion:	4
Subsystem:	Windows GUI
FileVersionNumber:	0.0.0.0
ProductVersionNumber:	0.0.0.0
FileFlagsMask:	0x003f
FileFlags:	(none)
FileOS:	Win32
ObjectFileType:	Executable application
FileSubtype:	-
LanguageCode:	Neutral
CharacterSet:	Unicode
Comments:	This installation was built with Inno Setup.
CompanyName:	Drive Software Company
FileDescription:	Butterfly on Desktop Setup
FileVersion:	
LegalCopyright:	
ProductName:	Butterfly on Desktop
ProductVersion:	

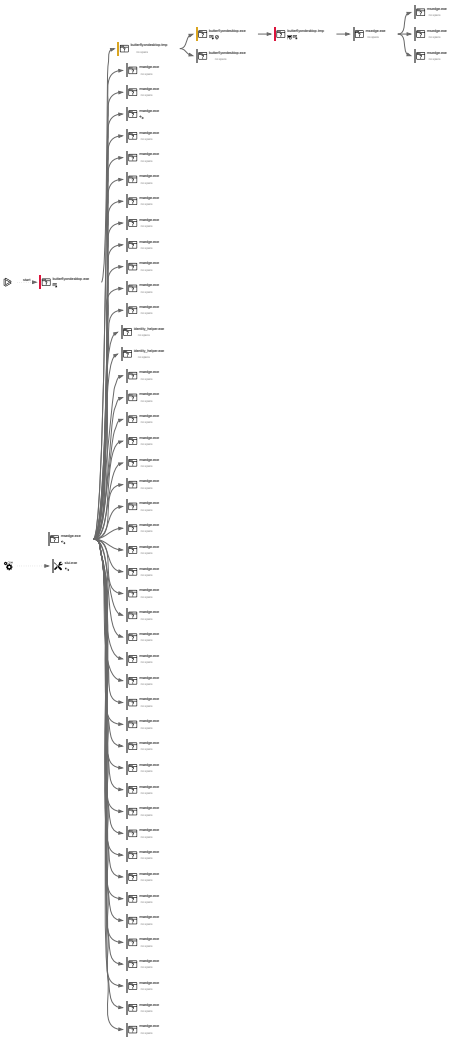
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
184	56	2	2

Behavior graph



Specs description

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

Process information

PID	CMD	Path	Indicators	Parent process
2392	"C:\Users\admin\Desktop\butterflyondesktop.exe"	C:\Users\admin\Desktop\butterflyondesktop.exe		explorer.exe

Information

User:	admin	**Company:**	Drive Software Company
Integrity Level:	MEDIUM	**Description:**	Butterfly on Desktop Setup
Exit code:	0	**Version:**	

5544	"C:\Users\admin\AppData\Local\Temp\is-DOT2Q.tmp\butterflyondesktop.tmp" /SL5="$A02D2,2719719,54272,C:\Users\admin\Desktop\butterflyondesktop.exe"	C:\Users\admin\AppData\Local\Temp\is-DOT2Q.tmp\butterflyondesktop.tmp	—	butterflyondesktop.exe

Information

User: admin **Integrity Level:** MEDIUM
Description: Setup/Uninstall **Exit code:** 0
Version: 51.52.0.0

1164	"C:\Users\admin\Desktop\butterflyondesktop.exe" /SPAWNWND=$802AE /NOTIFYWND=$A02D2	C:\Users\admin\Desktop\butterflyondesktop.exe		butterflyondesktop.tmp

Information

User: admin **Company:** Drive Software Company
Integrity Level: HIGH **Description:** Butterfly on Desktop Setup
Exit code: 0 **Version:**

1228	"C:\Users\admin\AppData\Local\Temp\is-DBAQS.tmp\butterflyondesktop.tmp" /SL5="$40310,2719719,54272,C:\Users\admin\Desktop\butterflyondesktop.exe" /SPAWNWND=$802AE /NOTIFYWND=$A02D2	C:\Users\admin\AppData\Local\Temp\is-DBAQS.tmp\butterflyondesktop.tmp		butterflyondesktop.exe

Information

User: admin **Integrity Level:** HIGH
Description: Setup/Uninstall **Exit code:** 0
Version: 51.52.0.0

5680	"C:\Program Files (x86)\Butterfly on Desktop\ButterflyOnDesktop.exe"	C:\Program Files (x86)\Butterfly on Desktop\ButterflyOnDesktop.exe	—	butterflyondesktop.tmp

Information

User: admin **Integrity Level:** MEDIUM

6040	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument http://freedesktopsoft.com/butterflyondesktoplike.html	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	butterflyondesktop.tmp

Information

User: admin **Company:** Microsoft Corporation
Integrity Level: HIGH **Description:** Microsoft Edge
Exit code: 1 **Version:** 122.0.2365.59

6768	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=122.0.6261.70 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 "--annotation=prod=Microsoft Edge" --annotation=ver=122.0.2365.59 --initial-client-data=0x240,0x260,0x318,0x264,0x320,0x7ffc89dd5fd8,0x7ffc89dd5fe4,0x7ffc89dd5ff0	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

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

3884	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=2408 --field-trial-handle=2360,i,16927040229595619545,4910122868638934882,262144 --variations-seed-version /prefetch:2	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

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

3676	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=2664 --field-trial-handle=2360,i,16927040229595619545,4910122868638934882,262144 --variations-seed-version /prefetch:3	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

User: admin **Company:** Microsoft Corporation

Integrity Level:	HIGH	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	122.0.2365.59

1328 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --flag-switches-begin --flag-switches-end --do-not-de-elevate --single-argument http://freedesktopsoft.com/butterflyondesktoplike.html — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe ↪ explorer.exe

Information

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

736 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\admin\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=122.0.6261.70 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 "--annotation=prod=Microsoft Edge" --annotation=ver=122.0.2365.59 --initial-client-data=0x298,0x29c,0x2a0,0x28c,0x290,0x7ffc89dd5fd8,0x7ffc89dd5fe4,0x7ffc89dd5ff0 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

5544 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=2432 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992,262144 --variations-seed-version /prefetch:2 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

5332 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=2720 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992,262144 --variations-seed-version /prefetch:3 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe ↪ msedge.exe

Information

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

1628 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=2756 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992,262144 --variations-seed-version /prefetch:8 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

6512 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=6 --mojo-platform-channel-handle=3532 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992,262144 --variations-seed-version /prefetch:1 — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

2552 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --mojo-platform- — C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

channel-handle=3736 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:1

Information

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

7192	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --extension-process --renderer-sub-type=extension --no-appcompat-clear --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=7 --mojo-platform-channel-handle=4188 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:2	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

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

7200	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=4460 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

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

7516	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=9 --mojo-platform-channel-handle=4712 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

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

7672	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.mojom.AssetStoreService --lang=en-US --service-sandbox-type=asset_store_service --no-appcompat-clear --mojo-platform-channel-handle=5372 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

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

7684	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity_extraction_service.mojom.Extractor --lang=en-US --service-sandbox-type=entity_extraction --onnx-enabled-for-ee --no-appcompat-clear --mojo-platform-channel-handle=5392 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

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

7696	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5564 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe

Information

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

7808	"C:\Program Files (x86)\Microsoft\Edge\Application\122.0.2365.59\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=5860 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\122.0.2365.59\identity_helper.exe	–	msedge.exe

Information

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

7844	"C:\Program Files (x86)\Microsoft\Edge\Application\122.0.2365.59\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=5860 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\122.0.2365.59\identity_helper.exe	–	msedge.exe

Information

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

7908	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5960 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

7948	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5968 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

7956	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6120 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

8024	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5980 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

8032	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6288 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

8144	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5964 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

8184	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6016 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

7296	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=6012 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

7304	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-sandbox-type=none --no-appcompat-clear --mojo-platform-channel-handle=6052 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

6972	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6012 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

7772	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=24 --mojo-platform-channel-handle=6044 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:1	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

7940	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6632 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

Exit code: 0 Version: 122.0.2365.59

7908 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_xpay_wallet.mojom.EdgeXPayWalletService --lang=en-US --service-sandbox-type=utility --no-appcompat-clear --mojo-platform-channel-handle=6664 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

8000 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6040 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

7960 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6796 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

8088 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6632 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

8032 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6008 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

3300 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6748 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

5744 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6316 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

2192 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --service-sandbox-type=none --ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=33 --mojo-platform-channel-handle=2812 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:1 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

1348 C:\WINDOWS\System32\slui.exe -Embedding C:\Windows\System32\slui.exe svchost.exe

Information

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

208 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=edge_search_indexer.mojom.SearchIndexerInterfaceBroker --lang=en-US --service-sandbox-type=search_indexer --message-loop-type-ui --no-appcompat-clear --mojo-platform-channel-handle=6944 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

5232 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6408 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

1012 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5536 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

8004 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=4168 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

8040 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=4180 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe — msedge.exe

Information

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

8084	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=4528 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

6112	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=6956 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

4728	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5824 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

7724	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=788 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

6640	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --disable-gpu-sandbox --use-gl=disabled --gpu-vendor-id=5140 --gpu-device-id=140 --gpu-sub-system-id=0 --gpu-revision=0 --gpu-driver-version=10.0.19041.3636 --no-appcompat-clear --gpu-preferences=WAAAAAAAAADoAAAMAAAAAAAAAAAAAAAAABgAAAAAA4AAAAAAAAAAAAAABEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAAAA== --mojo-platform-channel-handle=6064 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

7576	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --no-appcompat-clear --mojo-platform-channel-handle=5244 --field-trial-handle=2444,i,14986964373875403040,2253048509345367992, 262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

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

Registry activity

Total events	Read events	Write events	Delete events
9 282	9 240	42	0

Modification events

(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	Publisher
Value:	Drive Software Company		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	URLInfoAbout
Value:	http://www.freedesktopsoft.com		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	HelpLink
Value:	http://www.drive-software.com		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	URLUpdateInfo
Value:	http://www.drive-software.com		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	NoModify
Value:	1		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	NoRepair
Value:	1		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	InstallDate
Value:	20250305		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	EstimatedSize
Value:	6857		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation:	write	**Name:**	ButterflyOnDesktop
Value:			
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	Inno Setup: Setup Version
Value:	5.4.2 (a)		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	Inno Setup: App Path
Value:	C:\Program Files (x86)\Butterfly on Desktop		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	InstallLocation
Value:	C:\Program Files (x86)\Butterfly on Desktop\		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	Inno Setup: Icon Group
Value:	Butterfly on Desktop		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	Inno Setup: User
Value:	admin		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	Inno Setup: Selected Tasks
Value:			
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	Inno Setup: Deselected Tasks
Value:	butterflyondesktop		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	Inno Setup: Language
Value:	eng		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	DisplayName
Value:	Butterfly on Desktop 1.0		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	UninstallString
Value:	"C:\Program Files (x86)\Butterfly on Desktop\unins000.exe"		
(PID) Process:	(1228) butterflyondesktop.tmp	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Butterfly on Desktop_is1
Operation:	write	**Name:**	QuietUninstallString

Value: "C:\Program Files (x86)\Butterfly on Desktop\unins000.exe" /SILENT

(PID) Process: (1228) butterflyondesktop.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation: write **Name:** SlowContextMenuEntries
Value: 6024B221EA3A6910A2DC08002B30309D0A010000BD0E0C47735D584D9CEDE91E22E23282770100000114020000000000C000000000000468D0000006078A409B011A54DAFA526D86198A780390100009AD298B2EDA6DE11BA8CA68E55D895936E000000

(PID) Process: (1228) butterflyondesktop.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (1228) butterflyondesktop.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (1228) butterflyondesktop.tmp **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (6040) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** failed_count
Value: 0

(PID) Process: (6040) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** state
Value: 2

(PID) Process: (6040) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** state
Value: 1

(PID) Process: (1328) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** failed_count
Value: 0

(PID) Process: (1328) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** state
Value: 2

(PID) Process: (1328) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** state
Value: 1

(PID) Process: (6040) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\StabilityMetrics
Operation: write **Name:** user_experience_metrics.stability.exited_cleanly
Value: 0

(PID) Process: (6040) 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: 42CCC8D2348E2F00

(PID) Process: (1328) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\StabilityMetrics
Operation: write **Name:** user_experience_metrics.stability.exited_cleanly
Value: 0

(PID) Process: (1328) 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: 0DF6CFD2348E2F00

(PID) Process: (1328) 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: E464D6D2348E2F00

(PID) Process: (1328) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\656070
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {CF3D9AD7-A5AA-46E4-A13D-6C5DC57648C6}

(PID) Process: (1328) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\656070
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {D66E2092-D1FD-412B-8D8D-25B632F2E1F9}

(PID) Process: (1328) 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: 9187FFD2348E2F00

(PID) Process: (1328) 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: (1328) 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: (1328) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\656070
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {CE2BEC5E-9463-4119-873B-09432185A08D}

(PID) Process: (1328) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\Profiles
Operation: write **Name:** EnhancedLinkOpeningDefault
Value: Default

Files activity

Executable files	Suspicious files	Text files	Unknown types
20	317	51	0

Dropped files

PID	Process	Filename	Type
1164	butterflyondesktop.exe	C:\Users\admin\AppData\Local\Temp\is-DBAQS.tmp\butterflyondesktop.tmp **MD5:** C765336F0DCF4EFDCC2101EED67CD30C **SHA256:** C5177FDC6031728E10141745CD69EDBC91C92D14411A2DEC6E8E8CAA4F74AB28	executable
2392	butterflyondesktop.exe	C:\Users\admin\AppData\Local\Temp\is-DOT2Q.tmp\butterflyondesktop.tmp **MD5:** C765336F0DCF4EFDCC2101EED67CD30C **SHA256:** C5177FDC6031728E10141745CD69EDBC91C92D14411A2DEC6E8E8CAA4F74AB28	executable
1228	butterflyondesktop.tmp	C:\Users\admin\AppData\Local\Temp\is-9RQQ1.tmp_isetup_setup64.tmp **MD5:** 4FF75F505FDDCC6A9AE62216446205D9 **SHA256:** A4C86FC4836AC728D7BD96E7915090FD59521A9E74F1D06EF8E5A47C8695FD81	executable
1228	butterflyondesktop.tmp	C:\Users\admin\AppData\Local\Temp\is-9RQQ1.tmp_isetup_RegDLL.tmp **MD5:** 0EE914C6F0BB93996C75941E1AD629C6 **SHA256:** 4DC09BAC0613590F1FAC8771D18AF5BE25A1E1CB8FDBF4031AA364F3057E74A2	executable
1228	butterflyondesktop.tmp	C:\Users\admin\AppData\Local\Temp\is-9RQQ1.tmp_isetup_shfoldr.dll **MD5:** 92DC6EF532FBB4A5C3201469A5B5EB63 **SHA256:** 9884E9D1B4F8A873CCBD81F8AD0AE257776D2348D027D811A56475E028360D87	executable
1228	butterflyondesktop.tmp	C:\Program Files (x86)\Butterfly on Desktop\is-08KOI.tmp **MD5:** 1FEE4DB19D9F5AF7834EC556311E69DD **SHA256:** 3D550C908D5A8DE143C5CD5F4FE431528CD5FA20B77F4605A9B8CA063E83FC36	executable
1228	butterflyondesktop.tmp	C:\Program Files (x86)\Butterfly on Desktop\unins000.exe **MD5:** 1FEE4DB19D9F5AF7834EC556311E69DD **SHA256:** 3D550C908D5A8DE143C5CD5F4FE431528CD5FA20B77F4605A9B8CA063E83FC36	executable
1228	butterflyondesktop.tmp	C:\Program Files (x86)\Butterfly on Desktop\is-Q55JE.tmp **MD5:** 81AAB57E0EF37DDFF02D0106CED6B91E **SHA256:** A70F9E100DDDB177F68EE7339B327A20CD9289FAE09DCDCE3DBCBC3E86756287	executable
1228	butterflyondesktop.tmp	C:\Program Files (x86)\Butterfly on Desktop\is-2CD52.tmp **MD5:** 81AAB57E0EF37DDFF02D0106CED6B91E **SHA256:** A70F9E100DDDB177F68EE7339B327A20CD9289FAE09DCDCE3DBCBC3E86756287	executable
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old~RF110d0d.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old~RF110d0d.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old~RF110d0d.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old **MD5:** — **SHA256:** —	—
1228	butterflyondesktop.tmp	C:\Program Files (x86)\Butterfly on Desktop\ButterflyOnDesktop.exe **MD5:** 81AAB57E0EF37DDFF02D0106CED6B91E **SHA256:** A70F9E100DDDB177F68EE7339B327A20CD9289FAE09DCDCE3DBCBC3E86756287	executable
1228	butterflyondesktop.tmp	C:\Program Files (x86)\Butterfly on Desktop\is-VURLH.tmp **MD5:** F68621DA9CCBE320AEBB5807C6F733CB **SHA256:** 0479A712A54ADA76EAF0BC5F3B57C764880D1540CBE266724D35C4DCBF40E4E2	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old~RF110d1c.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old **MD5:** — **SHA256:** —	—
1228	butterflyondesktop.tmp	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Butterfly on Desktop\Butterfly on Desktop.lnk	binary

		MD5: A66C55CA2FD16507241E4B9A826D275E	**SHA256:** 94153B2A6BD50437EA48AA2747C1F32FB5A05A7235A6C958F59D16BCE385474B
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old~RF110d1c.TMP **MD5:** —	— **SHA256:** —
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old **MD5:** —	— **SHA256:** —
1228	butterflyondesktop.tmp	C:\Program Files (x86)\Butterfly on Desktop\license.txt **MD5:** F68621DA9CCBE320AEBB5807C6F733CB	text **SHA256:** 0479A712A54ADA76EAF0BC5F3B57C764880D1540CBE266724D35C4DCBF40E4E2
6040	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Version **MD5:** C7E2197BAE099B13BBB3ADEB1433487D	text **SHA256:** 3460EEAF45D581DD43A6E4E17AF8102DDAFF5AEAA88B10099527CF85211629E9
6040	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\904a63ee-6cb2-4641-816b-ae290d4fe499.tmp **MD5:** A8DB753E0EA7E903D1047037879C8357	binary **SHA256:** 0CBDF48668927A807F308CC738FFD8149B91E6A22582BBE7CE08E59C1BB7B9CE
6040	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Variations **MD5:** 6971E42ED64D2BE125547F021EB852B1	binary **SHA256:** B46CFDC4106DF566F71AA34D6F10B53767C561DFD17DD07A5930A18E67BB344B
1228	butterflyondesktop.tmp	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Butterfly on Desktop\Uninstall Butterfly on Desktop.lnk **MD5:** A554EFD232B5E9C921B32B7BCC1BB04C	binary **SHA256:** 52CA0F5D21F37913A3650BB89AE38C775B2005E89157882DBEAB516699306BA5
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old~RF110d99.TMP **MD5:** —	— **SHA256:** —
1228	butterflyondesktop.tmp	C:\Program Files (x86)\Butterfly on Desktop\unins000.dat **MD5:** AE9752C876531E9D319C2C572C2EA49E	binary **SHA256:** 8BD22BF5E195BA0EDD0176D7B0A75C7B52BA96F16C33D8BCB180E1176808D961
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old **MD5:** —	— **SHA256:** —
6040	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\settings.dat **MD5:** 1E9E15EF6E531C4557100F20C9C76F01	binary **SHA256:** 46CB063CC268B69B172660F166C4394D5B4EDD802388B3EC16766DEBDB9F86C3
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\570fe51f-49a0-4913-822e-fdcb1fcd2647.tmp **MD5:** 912AF2544D3374C71E3ED977E45FAF55	binary **SHA256:** 214B40EDA9479B8A0B3D655F7A09FDF3B155A7D0132C93A8A86BEBDE731ACE9E
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old~RF110ced.TMP **MD5:** C5C8E14929BCE261B2B5B899CB479AF7	text **SHA256:** 73DBFF8A366CFF6972A38C091782EF62C89E28FDA1423A47448A60343F921754
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old~RF110ced.TMP **MD5:** 92941BAD29B823669F85E6F7352F04EB	text **SHA256:** 19E674BF425E68E8B1C1242017BB22044BA558B1D5644F5D4EBA973AF39BABAA
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old **MD5:** 1AF1D1ED27A40F9FDA977B6C353EC48B	text **SHA256:** 01B66ED195749BF7909E0B655A6C4C6AFDECD665D7304653D09CD538191CC50A
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old **MD5:** 798EBA8558D3655BC5D2B61984B3BF12	text **SHA256:** 04EB76D36567C4FD801C5583AA34A18A081D9030BAE3034D8F81D419A797221D
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old~RF110d0d.TMP **MD5:** 818E5512B63AF7BC7B8363A92D905712	text **SHA256:** ECD4298AE18D0B60EA5F0B3B04761F740B51B18B0D69B42CEF028463A7A46780
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old **MD5:** FF65CBE0D511D23B79B630DD40BA28B6	text **SHA256:** 0BAFE077764110A681D8E15801BDAA10395BCFE9087FFF703BA3A83CAF73ADF0
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\todelete_fc3192cd274a0b5a **MD5:** 95FC65CACF599A197741EB36DEB0F8AE	binary **SHA256:** B84BDA5415D69DA598F2015A9BFDB024727F3DE3F0E9E6B16FDD7533026A5565
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\temp-index **MD5:** 01F0B29822F7C00694ABF3150276196A	binary **SHA256:** C5CA04147E678498F16E8DED9EFB227591ABF40A3AFC5E65248D019D9B9198D9
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index **MD5:** 01F0B29822F7C00694ABF3150276196A	binary **SHA256:** C5CA04147E678498F16E8DED9EFB227591ABF40A3AFC5E65248D019D9B9198D9
6040	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF110b09.TMP **MD5:** 1051384B8864AC718AE413E9B1D309A5	binary **SHA256:** 3FC536607727B6030F7B4714D6E03B4CA040B2EBDBE81B74538F345432207360
6040	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State **MD5:** A8DB753E0EA7E903D1047037879C8357	binary **SHA256:** 0CBDF48668927A807F308CC738FFD8149B91E6A22582BBE7CE08E59C1BB7B9CE
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\ea8498ab-768a-4b32-b603-dce817ed1fd6.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D	binary **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\7a5e50c7-fdb8-441c-8c18-1776d8dcf7fb.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D	binary **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF110cde.TMP **MD5:** A8DB753E0EA7E903D1047037879C8357	binary **SHA256:** 0CBDF48668927A807F308CC738FFD8149B91E6A22582BBE7CE08E59C1BB7B9CE
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State **MD5:** 912AF2544D3374C71E3ED977E45FAF55	binary **SHA256:** 214B40EDA9479B8A0B3D655F7A09FDF3B155A7D0132C93A8A86BEBDE731ACE9E
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old **MD5:** A440B2B4E06AF56BCDC8AE0E4ABF7A0B	text **SHA256:** EE6899D4DEE495E71C452A696AE4C984ED4DA5BF5E43078BF5EF10210F95D318
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old~RF110e64.TMP	text

		MD5: CE118DF5F2969D979F3D0E779BACF798 **SHA256:** 830316C00FB44CBFCC6AFF55FBE014BAA63B20B9BAA1DCE9E43856911F4F357E	
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old **MD5:** 7959D8DB0CBADD0EA4A5F1CC4E5B5138 **SHA256:** 270CB1734B667CF46D5A0A3149F36BC8867E5A239B56B212908994381528CD59	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old~RF110e74.TMP **MD5:** C1C75CFDA95DA438E30077FF767A6FDF **SHA256:** CED5E0654E5732FDDB0AE882D981C3FA7171889874047821BDF00245DC8EA913	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old **MD5:** D95248482054CC3F9158A60D13CE0BCE **SHA256:** AF8C73D6599B0D7603D52E50A01CD7A6AF4F3D23C5023CDF26B81DC0C14E0609	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old~RF110e74.TMP **MD5:** A913CE23AF5CEF8D1CD91F60B37EFA59 **SHA256:** A84AD219E5E1144AE35FACE15704BD066CCA689BECD82500276C7A6C5484F82D	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old **MD5:** BB2F8FF0F266CFB047C8472B2ED83BA2 **SHA256:** A8A372371A7E0DCDD0CF009BB5A4C6B192DBE0D83408EA91251A8185790236C1	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old~RF110ee1.TMP **MD5:** 35D729BE231A18224EB4469BA4BAB0E3 **SHA256:** 0D5F32F9C261450E1EAD9B4B12A3CD580C93389D11EB5CB5EC373950D6AC87FE	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old **MD5:** 8C15B19DD1169F3CA1A561CAFD619C02 **SHA256:** 0A69BB99412A7E4F7205F73AEDD9AB5D810D1639967F441AD8F711E702C53C0F	text
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\bd4a0ebf-a907-4eb9-a714-217b91959e0b.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\5a2fe272-05e5-4fe0-ac82-afec9776ef8f.tmp **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports~RF110f9d.TMP **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old~RF111a4b.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_model_metadata_store\LOG.old~RF111a5b.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_model_metadata_store\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old~RF111a6b.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old~RF111a8a.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RF111a8a.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old~RF111ac8.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RF111ad8.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RF111ad8.TMP **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old **MD5:** — **SHA256:** —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF110db9.TMP **MD5:** 912AF2544D3374C71E3ED977E45FAF55 **SHA256:** 214B40EDA9479B8A0B3D655F7A09FDF3B155A7D0132C93A8A86BEBDE731ACE9E	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\arbitration_service_config.json **MD5:** 350ABC86EFB653D78BE8F2FA5D7BDB8C **SHA256:** C42FB154D987390FCCC0F63DAFCED2BA7242410BADF64D6FF5FDC2FB26D103C9	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports **MD5:** D751713988987E9331980363E24189CE **SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\1ed1edff-b899-4dfa-b27d-7048bb63b476.tmp	binary

		MD5: 5B0C44BAF5BA34C838FE424BE0EF72DD	**SHA256:** 77040B425E8529226B9B4FE7735C67189C344BE05172A114F493DAA8EFFB2666
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\load_statistics.db-wal	binary
		MD5: BF4DF2FBD0B5E126973135D932B9A318	**SHA256:** A662866F79311CE2D7454137814BD287AE3EFCE1C71D1D7CCC65D98B9AEAAC11
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old~RF110dc8.TMP	text
		MD5: 29F7449691899E3CFC14F94670812757	**SHA256:** 1D1DF03022CD740C76320CAC538DE55D4521FF4EA32CE83275C982F1B308BBC6
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5a2a7058cf8d1e56c20e6b19a7c48eb2386d141b.tbres	binary
		MD5: 7052671F6E8F43AC1372F66F90A43B9C	**SHA256:** 04BC1AC1227B4906F85B3B0A9FA059FEA91DE6E9E93AD6DF8CF95705B77CCA9D
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\e0495fde257df2ef62ee7e3fdb1ebb9d7ff72300.tbres	binary
		MD5: 1E30FF27CD1591112CBCCC9CDE6417AD	**SHA256:** 3CA32D5B501BC3729CA7D55E08CE849AD276F5E4E34EFB84289DE57AA0E3A34F
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\default_cloud_config.json	binary
		MD5: 18261EB12378081F939FB9415CA0C9E1	**SHA256:** 12BBEEC9A0AF9E3ED945B28B9B8EF89B2F897768D1BA3FFD6F3FBB42FA5BC556
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old~RF1118b5.TMP	text
		MD5: 1F7041F0A707168BF7733D1A2047492C	**SHA256:** DB748A5163B0AB1FF8F312BC376F6BC8F5F4907BBC6DC85ED07299C656F2F729
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old	text
		MD5: 90E7FBA78823C029EB63EEBE05CB6647	**SHA256:** C402019AD51200620B9C3040D984A4EC6FF336CFB22039E29B761BE2DD63ADEE
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old~RF1118e4.TMP	text
		MD5: 279162E139C357A4BBCFBCFDD7A00E88	**SHA256:** 6B09138C2640F10EE9B088C48A47210A8570C7DCB3CAF340BADE94AC97FE9A0A
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old	text
		MD5: BD715F079C51E8C4D9AADFEF70125BD9	**SHA256:** 3DDC987F3DD33EA96D8B1D4E805E3A2D3B84B44C5F8FF0F224791F3ABFE7EDD7
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old~RF111913.TMP	text
		MD5: F22D72EFC12605BD6816B1F8B7831571	**SHA256:** D2442EFEB93BB5FD6FCFBA845320E097340EE086F48B1615484815BBA82BE122
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old	text
		MD5: 5F3EEB8D3062277537ADC926892A6E0A	**SHA256:** 601234D6C9DE44AE76920A3FD2E7D5C21F01C65CE8778BC084D02D977A801581
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\e8ddd4cbd9c0504aace6ef7a13fa20d04fd52408.tbres	binary
		MD5: 908F773405FC52E850DF43FEEF7A77C3	**SHA256:** B26D81D80267C12A0F71D56DCCB811AC23837853074D5212D2F8DF42CD9B8627
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Browser	binary
		MD5: A397E5983D4A1619E36143B4D804B870	**SHA256:** 9C70F766D3B84FC2BB298EFA37CC9191F28BEC336329CC11468CFADBC3B137F4
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports~RF110f7e.TMP	text
		MD5: D751713988987E9331980363E24189CE	**SHA256:** 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\cv_debug.log	binary
		MD5: B185A10C32C75B7B09460E11F9FD7FA6	**SHA256:** 49137337993C80DCD234892F709548D23A19354F0A4D7DB30F64984C3F3A439D
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\d1076bf6-e15c-455f-9899-0d8ca53ea391.tmp	binary
		MD5: 4A164D87B3F685E409A55B31861F0AE2	**SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Platform Notifications\LOG.old~RF111b16.TMP	text
		MD5: 0BFBF23732791ECBD0B56480C3DE5152	**SHA256:** 87C47D0E2E511DE24F20573FD90202DDCBB0C626118129769122FA870B8DF61A
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps~RF111af7.TMP	binary
		MD5: 4A164D87B3F685E409A55B31861F0AE2	**SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old~RF111b84.TMP	—
		MD5: —	**SHA256:** —
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old	—
		MD5: —	**SHA256:** —
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps	binary
		MD5: 4A164D87B3F685E409A55B31861F0AE2	**SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Platform Notifications\LOG.old	text
		MD5: F8F8200E9DC617B01F93320DA6BB7870	**SHA256:** 9FD3E46AB3D926076563DBB90176D38DD5F1427DCD851AF539B019CA62BE9FB9
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\msedge_url_fetcher_1328_1748038254\GHBMNNJOOEKPMOECNNNILNNBDLOLHKHI_1_89_1_0.crx	binary
		MD5: EAE462C55EBA847A1A8B58E58976B253	**SHA256:** EBCDA644BCFBD0C9300227BAFDE696E8923DDB004B4EE619D7873E8A12EAE2AD
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000258	compressed
		MD5: 0E6652994F4DDA1B8980A7EBD3B5A7E8	**SHA256:** 93CC94D9696C6FF0BBE4BF2657654C25A805BF8F9E154035CB1AFC9CEAEC7561
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795\page_embed_script.js	binary
		MD5: 0396274AAF2EAE8917E5EB52CF69DFA4	**SHA256:** 13E1562CD07FC06D692FDF1AA471E3CEAE3CF7C1E42C5345D430A947139A24D5
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795\service_worker_bin_prod.js	binary
		MD5: BC4DBD5B20B1FA15F1F1BC4A428343C9	**SHA256:** DFAD2626B0EAB3ED2F1DD73FE0AF014F60F29A91B50315995681CEAAEE5C9EA6
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795\dasherSettingSchema.json	binary
		MD5: 4EC1DF2DA46182103D2FFC3B92D20CA5	**SHA256:** 6C69CE0FE6FAB14F1990A320D704FEE362C175C00EB6C9224AA6F41108918CA6
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795\manifest.json	binary
		MD5: B0422D594323D09F97F934F1E3F15537	**SHA256:** 401345FB43CB0CEC5FEB5D838AFE84E0F1D0A1D1A299911D36B45E308F328F17
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795\offscreendocument_main.js	binary

		MD5: 01984DBFE92DF14DBD118C381A3D48F4 **SHA256:** 3A78B6FBC16F9FB27CE3ED650ABC31174263D762B71C028CC5D8F5427CBAB082	
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\lt\messages.json **MD5:** 8047409DCC27BFCC97B3ABCE6DAB20EF **SHA256:** B42EBFE071EF0EC4B4B6553ABF3A2C36B19792C238080A6FBC19D804D1ACB61C	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\fi\messages.json **MD5:** 1D4778E02337674D7D0664B5E7DFCBBE **SHA256:** A822B0E66D04644D1CFBD2517736728438743162C3213F15D986E2DB85BD0213	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\es_419\messages.json **MD5:** 94BC2D5609F6D670E181E1FF0D041869 **SHA256:** E848603B7A73A88E3FE7BFFA20E83397F5D1E93E77BABB31473CC99E654A27B7	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\fil\messages.json **MD5:** F954B2E970DC96E5889499DB7392FD59 **SHA256:** 41CE6A7B18364EFECCED0419B42165D4F86C43643BBE1043014D4142CF86186A	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\en\messages.json **MD5:** 558659936250E03CC14B60EBF648AA09 **SHA256:** 2445CAD863BE47BB1C15B57A4960B7B0D01864E63CDFDE6395F3B2689DC1444B	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\km\messages.json **MD5:** B3699C20A94776A5C2F90AEF6EB0DAD9 **SHA256:** A6118F0A0DE329E07C01F53CD6FB4FED43E54C5F53DB4CD1C7F5B2B4D9FB10E6	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\sr\messages.json **MD5:** C2026342237E7686B1932AF5B54F8110 **SHA256:** A3EB276FBD19DCE2B00DB6937578B214B9E33D67487659FE0BF21A86225ECE73	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\de\messages.json **MD5:** 5DAF77AE7D2B7DBEF44C5CF7E19805EE **SHA256:** 22E2828BFDBB9C340E7806894AE0442BD6C8934F85FBB964295EDAD79FD27528	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\es\messages.json **MD5:** 59CB3A9999DFBD19C3E3098F3B067634 **SHA256:** 02168993A23E074E0800CBB338FE279F99EF420E326BF92916FFED83C1F06533	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\sw\messages.json **MD5:** 84EB1D6E827E40C578469EAAB778E368 **SHA256:** 2C6B42D122943DC0CA92A33074D1A607351D3BC7F9768E174617FA7011A3DE9F	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\en_CA\messages.json **MD5:** 558659936250E03CC14B60EBF648AA09 **SHA256:** 2445CAD863BE47BB1C15B57A4960B7B0D01864E63CDFDE6395F3B2689DC1444B	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\eu\messages.json **MD5:** 29A1DA4ACB4C9D04F080BB101E204E93 **SHA256:** A41670D52423BA69C7A65E7E153E7B9994E8DD0370C584BDA0714BD61C49C578	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\sl\messages.json **MD5:** 9CDFA5371F28427F129D200338C47494 **SHA256:** 75D018CC8525605DDC591F6BFE5BDAA2EFB164934E9D5438972651F8C818D581	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ne\messages.json **MD5:** 065EB4DE2319A4094F7C1C381AC753A0 **SHA256:** 160E1CD593C901C7291EA4ECBA735191D793DDFD7E9646A0560498627F61DA6F	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\te\messages.json **MD5:** 50AB4DEABAD394D13C265B8B80D9F9C3 **SHA256:** 90868A8A4A4DBF48770C14A161FAEA406EF9A453B75F4CB7A53C1B4E96A88599	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\hi\messages.json **MD5:** 4A9C9F947B479E5D89C38752AF3C70EA **SHA256:** 14895BF43CE9B76C0FF4F9AEF93DBE8BB6CA496894870CF0C007B189E0CEF00E	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\az\messages.json **MD5:** C603747B8578C1324DD262565F643E06 **SHA256:** 614470DA3C5034ACE649F1786BEAAAD2C94F4475BCC8858390B721F06FB7BF64	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ja\messages.json **MD5:** 113A674F2E4C66CC4D2A9C66ED77ADEA **SHA256:** C1094A1D8457E782F229910B70FC7AECE356AA779A423E869104946814660D35	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\zh_TW\messages.json **MD5:** B571E4CEFD96A2651FFB6621C4D3D1B4 **SHA256:** 16B8F7BE42B982D5AD9F638E71DA38D134394B9BAB9255F73CF514ABBFAAF146	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\et\messages.json **MD5:** B18007BFC2B55D2F5839A8912110B98D **SHA256:** 7CCC7B17BFE01C3C7DD33EFF8F80D0B57FC9B175815E766C9C1C1E893725E20F	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ta\messages.json **MD5:** 24626AD7B8058866033738380776F59B **SHA256:** 3FC7F56F6D6D514B32547509B39F6380FC786EFBCCA4B9859F204456CA2E7957	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\mr\messages.json **MD5:** 34CE3FA84E699BCE78E026D0F0A0C705 **SHA256:** 275E7FADB93A810328E3ADEAD8754DD0A19A062D5D20A872F7471FFAB47AA7B3	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\el\messages.json **MD5:** 32886978EF4B5231F921EB54E683EB10 **SHA256:** 728D8CBD71263680A4E41399DB65B3F2B8175D50CA630AFD30643CED9FFE831F	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\en_GB\messages.json **MD5:** C4E77421F3361277F7E3AA3472B5EB10 **SHA256:** C7255E9B784C4B8DF7DF7B78F33A5737A9AB7382F73465351597B1DA9B3D5FE7	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ru\messages.json **MD5:** F70662272A8FC9141A295A54002F644F **SHA256:** DF379187B7F6DE700E5C53420336E6B31B7DC31015F77B2B256256BCF9BE54B7	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\fr_CA\messages.json **MD5:** 681422E3FCF8711AF8EEFBB75A607C8E **SHA256:** AF889C1DEB6F9248961C2F8BA4307A8206D7163616A5B7455D17CEAD00068317	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\gu\messages.json **MD5:** 86DE754C2D6B550048C9D914E55B5FF0 **SHA256:** CC3E9077FCC9BD0DFC5DD3924C6C48B8345F32CEE24FCCC508C279F45B2ABE61	binary
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\zh_CN\messages.json **MD5:** E910D3F03F0349F5C8A6A541107375D5 **SHA256:** 3893C066A36FE95F06F3C49091A20290D4E071183755F40AF05455660BEDA2DC	binary

8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\en_US\messages.json	binary
		MD5: 64EAEB92CB15BF128429C2354EF22977	**SHA256:** 4F70ECA8E28541855A11EC7A4E6B3BC6DD16C672FF9B596ECFB7715BB3B5898C
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ms\messages.json	binary
		MD5: DB4D49231C88C11E8D8C3D71A9B7D3D4	**SHA256:** 9B32C491D0BFEBDCA1455F73C3C6F71796D433A39818C06C353DA588DE650F81
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\si\messages.json	binary
		MD5: B8A4FD612534A171A9A03C1984BB4BDD	**SHA256:** 54241EBE651A8344235CC47AFD274C080ABAEBC8C3A25AFB95D8373B6A5670A2
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\fa\messages.json	binary
		MD5: E578E08EE604158D674982BA060396FD	**SHA256:** E758273C25FBAD804FE884584E2797CAEFBBD1C2877DFD6F87AB1340CD25252E
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\is\messages.json	binary
		MD5: CAEB37F451B5B5E9F5EB2E7E7F46E2D7	**SHA256:** 943E61988C859BB088F548889F0449885525DD660626A89BA67B2C94CFBFBB1B
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\bn\messages.json	binary
		MD5: B1101FAC65CE2FAA3702E70FD88957D2	**SHA256:** 3E3CEAA214D8079B02C9C941635F5D45E621236D9C3F82E06AC604F0772670E8
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\pt_PT\messages.json	binary
		MD5: AA431EC252B4339A49D172C6B9292BA3	**SHA256:** 156FC7BA9B5728908E1A74950B97474F73D8F58933D345C8EEEA8284565C8357
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\hu\messages.json	binary
		MD5: FB8D08676AA88683F27A2759C5837529	**SHA256:** CF26310B073B0891996ECD761C6CB53F00193DEE524213A9FB34225D636EC4B7
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ml\messages.json	binary
		MD5: CE70315E2AAEDA0999DA38CC9FE65281	**SHA256:** 907F2709D1D3C8FA26294938F4080BC477E62281C4C50A082C22DB0195CDA663
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\my\messages.json	binary
		MD5: 342335A22F1886B8BC92008597326B24	**SHA256:** 243BEFBD6B67A21433DCC97DC1A728896D3A070DC20055EB04D644E1BB955FE7
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\da\messages.json	binary
		MD5: 0E451C9C8453577E513AABF630C275F2	**SHA256:** 94CDDB998C2C5AB40B6F074C359A60E6EEBAAA2D52A9649C22F4EA4C1B9936F2
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\id\messages.json	binary
		MD5: 3FEFE403F5F537D9A2D28AB36B2C1A94	**SHA256:** 35872A3343D4B4768FE4702A8DC18B749933E81210DB13466AD172BD2880F6EB
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\hr\messages.json	binary
		MD5: EB6C5133C1FE7F9E8E4449A917D185D9	**SHA256:** 985976B776E729835E047C81D3D731A6C488A6459AA8918DBC8EC808C0BF73A1
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ar\messages.json	binary
		MD5: C825621044E4D5C504404DAE9752285C	**SHA256:** 47652115CBB912907F405992FCFC64F987642158F0CB35C9D6E0D4742D833802
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\zu\messages.json	binary
		MD5: 71F916A64F98B6D1B5D1F62D297FDEC1	**SHA256:** EC78DDD4CCF32B5D76EC701A20167C3FBD146D79A505E4FB0421FC1E5CF4AA63
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\hy\messages.json	binary
		MD5: 55DE859AD778E0AA9D950EF505B29DA9	**SHA256:** 0B16E3F8BD904A767284345AE86A0A9927C47AFE89E05EA2B13AD80009BDF9E4
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\sv\messages.json	binary
		MD5: F008F729147F028A91E700008130DA52	**SHA256:** 5F4229D18E5606330146EE13BDF726E10C1E06CBB15368C47F1AE68ABE9CE4BA
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\nl\messages.json	binary
		MD5: D448E11801349AB5704DF8446FE3FA4C	**SHA256:** E98C5CFE277A338A938E7277DEEC132F5EA82A53EBDB65FF10E8A2FF548AC198
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\cy\messages.json	binary
		MD5: A86407C6F20818972B80B9384ACFBBED	**SHA256:** A482663292A913B02A9CDE4635C7C92270BF3C8726FD274475DC2C490019A7C9
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\gl\messages.json	binary
		MD5: CC31777E68B20F10A394162EE3CEE03A	**SHA256:** 9890710DF0FBF1DB41BCE41FE2F62424A3BD39D755D29E829744ED3DA0C2CE1D
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\no\messages.json	binary
		MD5: 66439BA3ED5BA0C702EF94793E15DE83	**SHA256:** B3ECE279943B28C8D855EC86AC1CE53BDFB6A709240D653508764493A75F7518
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\pt_BR\messages.json	binary
		MD5: 8E24EC937237F48AC98B27F47B688C90	**SHA256:** A6AD5D5FB7C90736E04F898970D2CC9D423415B54B8E572F18C05D6EBAF46F68
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\af\messages.json	binary
		MD5: 7BC8FED14870159B4770D2B43B95776B	**SHA256:** AA12205B108750CF9FA0978461A6D8881E4E80DA20A846D824DA4069D9C91847
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\zh_HK\messages.json	binary
		MD5: 524E1B2A370D0E71342D05DDE3D3E774	**SHA256:** 30F44CFAD052D73D86D12FA20CFC111563A3B2E4523B43F7D66D934BA8DACE91
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ko\messages.json	binary
		MD5: E71A91FE65DD32CAC3925CE639441675	**SHA256:** 57F81A5FCBD1FEFD6EC3CDD525A85B707B4EEAD532C1B3092DAAFD88EE9268EC
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\bg\messages.json	binary
		MD5: 361B516EDF253851044DAE6BAD6D9D6F	**SHA256:** 22BC37B47CE8A832F39701641DC358357676E9BE187A93A4C5D4B016E29238AE
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\kn\messages.json	binary
		MD5: F55CE2E64A06806B43816AB17D8EE623	**SHA256:** 5FA00C465C1C5EED4BEA860CEB78DA9419EA115347BA543DDB0076E5C188FEED
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\sk\messages.json	binary
		MD5: A46E08B45BE0532E461E007E894B94F4	**SHA256:** 5E886E7B616FBFF3671DAB632D1B6D8DCEEFF9004218485F1B911DCD8C9694A3
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\it\messages.json	binary

		MD5: 88A9ACD41521D1D00B870E2DA3044A88	**SHA256:** 3377A873DB531113D79919E7A89369A79A602BAC6AE09B9864B9378DC285F345
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\fr\messages.json	binary
		MD5: 85718FE4820C674C5305D33DFB5CBDDC	**SHA256:** 6713B69B6C9E80B03E0A9D4A7D158197B0C7EC8A853C64C0AF0B1A05CE54D74C
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\lv\messages.json	binary
		MD5: 20FA89BA92628F56D36AE5BD0909CB15	**SHA256:** 80D64F03DC2CC5283FAF1354E05D3C3CB8F0CC54B3E76FDAE3AD8A09C9D5F267
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ur\messages.json	binary
		MD5: F6E8FCA4FD1A7AF320D4D30D6055FA6D	**SHA256:** 504549057A6A182A404C36112D2450864A6CB4574CD0E8F435CA556FAC52AB0A
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ka\messages.json	binary
		MD5: 83F81D30913DC4344573D7A58BD20D85	**SHA256:** 30898BBF51BDD58DB397FF780F061E33431A38EF5CFC288B5177ECF76B399F26
7684	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\domains_config.json	binary
		MD5: B5C7F7DAD1B86E0C2FEEA225F41F74A2	**SHA256:** A38BEC1B40870CA0B33218384039AC98C101CEEF402564846F8053C758FBC0AC
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\tr\messages.json	binary
		MD5: 3104BCD0D4AD6B47FE36F36C1B5AA333	**SHA256:** AC2894CEA6332450095A7F8FC9B97550DA87E4B4B6E6FB95DF1A1F49F25E0E35
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ro\messages.json	binary
		MD5: EE122CF26EBE1AD0CC733B117A89FF3B	**SHA256:** 4ECEDB9C1F3DD0D0E3AEB86146561B3D7E58656CBDBED1A39B91737B52EC7F2C
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\be\messages.json	binary
		MD5: 68884DFDA320B85F9FC5244C2DD00568	**SHA256:** DDF16859A15F3EB3334D6241975CA3988AC3EAFC3D96452AC3A4AFD3644C8550
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\am\messages.json	binary
		MD5: 83E0E58D0752FF7C3F888E6406413B84	**SHA256:** 64E01BC292BA2EA1699576FCC4453670475 20EE895E290CCEE20C24C9336D8EF
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\mn\messages.json	binary
		MD5: 83E7A14B7FC60D4C66BF313C8A2BEF0B	**SHA256:** 613D8751F6CC9D3FA319F4B7EA8B2BD3BED37FD077482CA825929DD7C12A69A8
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\kk\messages.json	binary
		MD5: 2D94A58795F7B1E6E43C9656A147AD3C	**SHA256:** 548DC6C96E31A16CE355DC55C64833B08EF3FBA8BF33149031B4A685959E3AF4
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\lo\messages.json	binary
		MD5: E20D6C27840B406555E2F5091B118FC5	**SHA256:** 89082FB05229826BC222F5D22C158235F025F0E6DF67FF135A18BD899E13BB8F
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\pl\messages.json	binary
		MD5: 10BA7FE4CAB38642419BE8FEF9E78178	**SHA256:** 6538F562BD1BAA828C0EF0ADC5F7C96B4A0EB7814E6B9A2B585E4D3B92B0E61D
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\th\messages.json	binary
		MD5: 0875B0BAD81161CCF2C16E13EE49AF9D	**SHA256:** D299AA0C4F29C5C8248A1C51AFDB7439F4CF7BC28EE02408A598F8AAD9F70810
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\vi\messages.json	binary
		MD5: 1E54AFBACCA335BE3A050920DDFBE863	**SHA256:** F1DA95E1D58E933050CD8A4FEA12F3D1B9A2759479FFDB74FDC1CFBF89568327
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\iw\messages.json	binary
		MD5: 26B1533C0852EE4661EC1A27BD87D6BF	**SHA256:** BBB81C32F482BA3216C9B1189C70CEF39CA8C2181AF3538FFA07B4C6AD52F06A
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\ca\messages.json	binary
		MD5: FBB841A2982166239D68907361F41F61	**SHA256:** DE6D7B7C2427EC4E738407D7834B71941F69166B030355E00F325FF1391DF5A1
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795\128.png	image
		MD5: D056CEC3B05D6A863DDFA7EE4C1C9F0C	**SHA256:** FF702CA753A7E3B75F9D9850CC9343E28E8D60F8005A2C955C8AC2105532B2C9
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\cs\messages.json	binary
		MD5: 48663A88DCF0EF6C9FADE9BEE4935B91	**SHA256:** 5A701D67910BA6C7CCEDC26E02FA707CC86A1BE57CD7D36290A3D268732A42C7
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\uk\messages.json	binary
		MD5: AE938164F7AC0E7C7F120742DE2BEB1E	**SHA256:** 08978A1425DEC304483BBB7DD0E55A7D850C4561ABD41BAC1BE5D93D70465174
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795\offscreendocument.html	html
		MD5: B747B5922A0BC74BBF0A9BC59DF7685F	**SHA256:** B9FA2D52A4FFABB438B56184131B893B04655B01F336066415D4FE839EFE64E7
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_metadata\verified_contents.json	text
		MD5: 8F99E1EF2AFC5F73D9391C248A0390AA	**SHA256:** D57215628AF1ECD1ECD8F83DA69245161E4E0A2CE24846B2FFF6B35DA232709B
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795\manifest.fingerprint	text
		MD5: 960A6760446FEDA24DB425BDB4123F21	**SHA256:** 7E69ED2C93D3A4CF2565D2712188A291A8A73470A1792039E760E01C174545D6
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\c74e7b5e-40e6-4807-9027-f09e781198d6.tmp	binary
		MD5: 5058F1AF8388633F609CADB75A75DC9D	**SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL\128.png	image
		MD5: 35696ABA596D5B8619A558DD05B4AD40	**SHA256:** 75DA533888189D13FC340D40637B9FC07A3F732E3FCF33EC300F4C7268790A62
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\af\messages.json	binary
		MD5: 12403EBCCE3AE8287A9E823C0256D205	**SHA256:** B40BDE5B612CFFF936370B32FB0C58CC205FC89937729504C6C0B527B60E2CBA
8144	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2034159795_locales\pa\messages.json	binary
		MD5: 97F769F51B83D35C260D1F8CFD7990AF	**SHA256:** BBD37D41B7DE6F93948FA2437A7699D4C30A3C39E736179702F212CB36A3133C
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\am\messages.json	binary
		MD5: 9721EBCE89EC51EB2BAEB4159E2E4D8C	**SHA256:** 3D0361A85ADFCD35D0DE74135723A75B646965E775188F7DCDD35E3E42DB788E

1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ar\messages.json	binary
		MD5: 3EC93EA8F8422FDA079F8E5B3F386A73	**SHA256:** ABD0919121956AB535E6A235DE67764F46CFC944071FCF2302148F5FB0E8C65A
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\az\messages.json	binary
		MD5: 9A798FD298008074E59ECC253E2F2933	**SHA256:** 628145F4281FA825D75F1E332998904466ABD050E8B0DC8BB9B6A20488D78A66
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\bg\messages.json	binary
		MD5: 2E6423F38E148AC5A5A041B1D5989CC0	**SHA256:** AC4A8B5B7C0B0DD1C07910F30DCFBDF1BCB701CFCFD182B6153FD3911D566C0E
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\bn\messages.json	binary
		MD5: 651375C6AF22E2BCD228347A45E3C2C9	**SHA256:** 1DBF38E425C5C7FC39E8077A837DF0443692463BA1FBE94E288AB5A93242C46E
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ca\messages.json	binary
		MD5: D177261FFE5F8AB4B3796D26835F8331	**SHA256:** D6E65238187A430FF29D4C10CF1C46B3F0FA4B91A5900A17C5DFD16E67FFC9BD
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\cs\messages.json	binary
		MD5: CCB00C63E4814F7C46B06E4A142F2DE9	**SHA256:** 21AE66CE537095408D21670585AD12599B0F575FF2CB3EE34E3A48F8CC71CFAB
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\da\messages.json	binary
		MD5: B922F7FD0E8CCAC31B411FC26542C5BA	**SHA256:** 48847D57C75AF51A44CBF8F7EF1A4496C2007E58ED56D340724FDA1604FF9195
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\de\messages.json	binary
		MD5: D116453277CC860D196887CEC6432FFE	**SHA256:** 36AC525FA6E28F18572D71D75293970E0E1EAD68F358C20DA4FDC643EEA2C1C5
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\el\messages.json	binary
		MD5: 9ABA4337C670C6349BA38FDDC27C2106	**SHA256:** 37CA6AB271D6E7C9B00B846FDB969811C9CE7864A85B5714027050795EA24F00
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\en\messages.json	binary
		MD5: 07FFBE5F24CA348723FF8C6C488ABFB8	**SHA256:** 6895648577286002F1DC9C3366F558484EB7020D52BBF64A296406E61D09599C
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\en_US\messages.json	binary
		MD5: 578215FBB8C12CB7E6CD73FBD16EC994	**SHA256:** 102B586B197EA7D6EDFEB874B97F95B05D229EA6A92780EA8544C4FF1E6BC5B1
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\es\messages.json	binary
		MD5: F61916A206AC0E971CDCB63B29E580E3	**SHA256:** 2008F4FAAB71AB8C76A5D8811AD40102C380B6B929CE0BCE9C378A7CADFC05EB
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\es_419\messages.json	binary
		MD5: 535331F8FB98894877811B14994FEA9D	**SHA256:** 90A560FF82605DB7EDA26C90331650FF9E42C0B596CEDB79B23598DEC1B4988F
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\et\messages.json	binary
		MD5: 64204786E7A7C1ED9C241F1C59B81007	**SHA256:** CC31B877238DA6C1D51D9A6155FDE565727A1956572F466C387B7E41C4923A29
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\fa\messages.json	binary
		MD5: 097F3BA8DE41A0AAF436C783DCFE7EF3	**SHA256:** 7C4C09D19AC4DA30CC0F7F521825F44C4DFBC19482A127FBFB2B74B3468F48F1
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\fi\messages.json	binary
		MD5: B38CBD6C2C5BFAA6EE252D573A0B12A1	**SHA256:** 2D752A5DBE80E34EA9A18C958B4C754F3BC10D63279484E4DF5880B8FD1894D2
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\en_CA\messages.json	binary
		MD5: 07FFBE5F24CA348723FF8C6C488ABFB8	**SHA256:** 6895648577286002F1DC9C3366F558484EB7020D52BBF64A296406E61D09599C
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\fr\messages.json	binary
		MD5: A58C0EEBD5DC6BB5D91DAF923BD3A2AA	**SHA256:** 0518287950A8B010FFC8D52554EB82E5D93B6C3571823B7CECA898906C11ABCC
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\fr_CA\messages.json	binary
		MD5: 6CAC04BDCC09034981B4AB567B00C296	**SHA256:** 4CAA46656ECC46A420AA98D3307731E84F5AC1A89111D2E808A228C436D83834
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\gl\messages.json	binary
		MD5: 6BAAFEE2F718BEFBC7CD58A04CCC6C92	**SHA256:** 0CF098DFE5BBB46FC0132B3CF0C54B06B4D2C8390D847EE2A65D20F9B7480F4C
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\gu\messages.json	binary
		MD5: BC7E1D09028B085B74CB4E04D8A90814	**SHA256:** FE8218DF25DB54E633927C4A1640B1A41B8E6CB3360FA386B5382F833B0B237C
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\hi\messages.json	binary
		MD5: 98A7FC3E2E05AFFFC1CFE4A029F47476	**SHA256:** D2D1AFA224CDA388FF1DC8FAC24CDA228D7CE09DE5D375947D7207FA4A6C4F8D
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\hr\messages.json	binary
		MD5: 25CDFF9D60C5FC4740A48EF9804BF5C7	**SHA256:** 73E6E246CEEAB9875625CD4889FBF931F93B7B9DEAA11288AE1A0F8A6E311E76
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\hu\messages.json	binary
		MD5: 8930A51E3ACE3DD897C9E61A2AEA1D02	**SHA256:** 958C0F664FCA20855FA84293566B2DDB7F297185619143457D6479E6AC81D240
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\id\messages.json	binary
		MD5: 34D6EE258AF9429465AE6A078C2FB1F5	**SHA256:** E3C86DDD2EFEBE88EED8484765A9868202546149753E03A61EB7C28FD62CFCA1
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\it\messages.json	binary
		MD5: 0D82B734EF045D5FE7AA680B6A12E711	**SHA256:** F41862665B13C0B4C4F562EF1743684CCE29D4BCF7FE3EA494208DF253E33885
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ja\messages.json	binary
		MD5: 15EC1963FC113D4AD6E7E59AE5DE7C0A	**SHA256:** 34AC08F3C4F2D42962A3395508818B48CA323D22F498738CC9F09E78CB197D73
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\kn\messages.json	binary
		MD5: 38BE0974108FC1CC30F13D8230EE5C40	**SHA256:** 30078EF35A76E02A400F03B3698708A0145D9B57241CC4009E010696895CF3A1
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\en_GB\messages.json	binary

		MD5: 3734D498FB377CF5E4E2508B8131C0FA	**SHA256:** AB5CDA04013DCE0195E80AF714FBF3A67675283768FFD062CF3CF16EDB49F5D4
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ko\messages.json	binary
		MD5: F3E59EEEB007144EA26306C20E04C292	**SHA256:** C52D9B955D229373725A6E713334BBB31EA72EFA9B5CF4FBD76A566417B12CAC
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\lt\messages.json	binary
		MD5: 970544AB4622701FFDF66DC556847652	**SHA256:** 5DFCBD4DFEAEC3ABE973A78277D3BD02CD77AE635D5C8CD1F816446C61808F59
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\lv\messages.json	binary
		MD5: A568A58817375590007D1B8ABCAEBF82	**SHA256:** 0621DE9161748F45D53052ED8A430962139D7F19074C7FFE7223ECB06B0B87DB
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ml\messages.json	binary
		MD5: 4717EFE4651F94EFF6ACB6653E868D1A	**SHA256:** 22CA9415E294D9C3EC3384B9D08CDAF5164AF73B4E4C251559E09E529C843EA6
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\mr\messages.json	binary
		MD5: 3B98C4ED8874A160C3789FEAD5553CFA	**SHA256:** ADEB082A9C754DFD5A9D47340A3DDCC19BF9C7EFA6E629A2F1796305F1C9A66F
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\fil\messages.json	binary
		MD5: FCEA43D62605860FFF41BE26BAD80169	**SHA256:** F51EEB7AAF5F2103C1043D520E5A4DE0FA75E4DC375E23A2C2C4AFD4D9293A72
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\nl\messages.json	binary
		MD5: 32DF72F14BE59A9BC9777113A8B21DE6	**SHA256:** F3FE1FFCB182183B76E1B46C4463168C746A38E461FD25CA91FF2A40846F1D61
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\no\messages.json	binary
		MD5: A1744B0F53CCF889955B95108367F9C8	**SHA256:** 21CEFF02B45A4BFD60D144879DFA9F427949A027DD49A3EB0E9E345BD0B7C9A8
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\pl\messages.json	binary
		MD5: B8D55E4E3B9619784AECA61BA15C9C0F	**SHA256:** E00FF20437599A5C184CA0C79546CB6500171A95E5F24B9B5535E89A89D3EC3D
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\pt_BR\messages.json	binary
		MD5: 608551F7026E6BA8C0CF85D9AC11F8E3	**SHA256:** A73EEA087164620FA2260D3910D3FBE302ED85F454EDB1493A4F287D42FC882F
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\pt_PT\messages.json	binary
		MD5: 0963F2F3641A62A78B02825F6FA3941C	**SHA256:** E93B8E7FB86D2F7DFAE57416BB1FB6EE0EEA25629B972A5922940F0023C85F90
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ro\messages.json	binary
		MD5: BED8332AB788098D276B448EC2B33351	**SHA256:** 085787999D78FADFF9600C9DC5E3FF4FB4EB9BE06D6BB19DF2EEF8C284BE7B20
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ru\messages.json	binary
		MD5: 51D34FE303D0C90EE409A2397FCA437D	**SHA256:** BE733625ACD03158103D62BC0EEF272CA3F265AC30C87A6A03467481A177DAE3
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\sk\messages.json	binary
		MD5: 8E55817BF7A87052F11FE554A61C52D5	**SHA256:** 903060EC9E76040B46DEB47BBB041D0B28A6816CB9B892D7342FC7DC6782F87C
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\sl\messages.json	binary
		MD5: BFAEFEFF32813DF91C56B71B79EC2AF4	**SHA256:** AAB9CF9098294A46DC0F2FA468AFFF7CA7C323A1A0EFA70C9DB1E3A4DA05D1D4
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\sr\messages.json	binary
		MD5: 7F5F8933D2D078618496C67526A2B066	**SHA256:** 4E8B69E864F57CDDD4DC4E4FAF2C28D496874D06016BC22E8D39E0CB69552769
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\sv\messages.json	binary
		MD5: 90D8FB448CE9C0B9BA3D07FB8DE6D7EE	**SHA256:** 64B1E422B346AB77C5D1C77142685B3FF7661D498767D104B0C24CB36D0EB859
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ta\messages.json	binary
		MD5: DCC0D1725AEAEAAF1690EF8053529601	**SHA256:** 6282BF9DF12AD453858B0B531C8999D5FD6251EB855234546A1B30858462231A
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\te\messages.json	binary
		MD5: 385E65EF723F1C4018EEE6E4E56BC03F	**SHA256:** 026C164BAE27DBB36A564888A796AA3F188AAD9E0C37176D48910395CF772CEA
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\th\messages.json	binary
		MD5: 64077E3D186E585A8BEA86FF415AA19D	**SHA256:** D147631B2334A25B8AA4519E4A30FB3A1A85B6A0396BC688C68DC124EC387D58
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\sw\messages.json	binary
		MD5: D0579209686889E079D87C23817EDDD5	**SHA256:** 0D20680B74AF10EF8C754FCDE259124A438DCE3848305B0CAF994D98E787D263
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ms\messages.json	binary
		MD5: 7D273824B1E22426C033FF5D8D7162B7	**SHA256:** 2824CF97513DC3ECC261F378BFD595AE95A5997E9D1C63F5731A58B1F8CD54F9
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\tr\messages.json	binary
		MD5: 76B59AAACC7B469792694CF3855D3F4C	**SHA256:** B9066A162BEE00FD50DC48C71B32B69DFFA362A01F84B45698B017A624F46824
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\uk\messages.json	binary
		MD5: 970963C25C2CEF16BB6F60952E103105	**SHA256:** 9FA26FF09F6ACDE2457ED366C0C4124B6CAC1435D0C4FD8A870A0C090417DA19
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ur\messages.json	binary
		MD5: 8B4DF6A9281333341C939C244DDB7648	**SHA256:** 5DA836224D0F3A96F1C5EB5063061AAD837CA9FC6FED15D19C66DA25CF56F8AC
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\ne\messages.json	binary
		MD5: B1083DA5EC718D1F2F093BD3D1FB4F37	**SHA256:** E6ED0A023EF31705CCCBAF1E07F2B4B2279059296B5CA973D2070417BA16F790
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\vi\messages.json	binary
		MD5: 773A3B9E708D052D6CBAA6D55C8A5438	**SHA256:** 597C5F32BC999746BC5C2ED1E5115C523B7EB1D33F81B042203E1C1DF4BBCAFE
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\zh_CN\messages.json	binary
		MD5: 3E76788E17E62FB49FB5ED5F4E7A3DCE	**SHA256:** E72D0BB08CC3005556E95A498BD737E7783BB0E56DCC202E7D27A536616F5EE0

1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\scoped_dir1328_1128135012\CRX_INSTALL_locales\zh_TW\messages.json **MD5:** 0E60627ACFD18F44D4DF469D8DCE6D30 **SHA256:** F94C6DDEDF067642A1AF18D629778EC65E02B6097A8532B7E794502747AEB008	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Rules\LOG.old~RF111e81.TMP **MD5:** 8FFDD5580E3C319A0F8610CF97BBD782 **SHA256:** 8391517B70D41DA3CBE3E1E51E275A3DE6514C8F9DA5C4BA2F0BD1859BCB0106	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Rules\LOG.old **MD5:** E30B48D8AE2479EF529F0AB65CB1F975 **SHA256:** DEE4176B1D6450A9A96383F5007E77C4C7D8CD43115F5953C139926D20C9591E	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Scripts\LOG.old~RF111e91.TMP **MD5:** 61A40A6640E8F12CB329C1E36223E2C9 **SHA256:** B311101250AAE9917310821EFCB0D9E43FC4B29AA2BE0E6C8CF066DA8FA730D9	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension Scripts\LOG.old **MD5:** D392F4191F0DFF78511FBDE7E3E08BF6 **SHA256:** 2AEA14504BC6FD1BD5869775B27795446DE98AED4A5C8D8D467E2F542F935A5E	text
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\96186517-c496-4556-9140-c978043c1774.tmp **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries~RF1135f1.TMP **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries **MD5:** 20D4B8FA017A12A108C87F540836E250 **SHA256:** 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RF1138ef.TMP **MD5:** FDF62CB6FD1CDDE50143B56A62355BF1 **SHA256:** 1F2755713752AB9B63A512BF29F2B3798F2C5372AF699EDCC6C7F72D457C9A7E	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State **MD5:** 54F6C9CFF7D91E723B2147B978E8FFA2 **SHA256:** 87BC6C4815CB7A6A01362095B29FB2AF8E7FB00CBADFC860559A96F0E13C8B30	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF11346b.TMP **MD5:** 5B0C44BAF5BA34C838FE424BE0EF72DD **SHA256:** 77040B425E8529226B9B4FE7735C67189C344BE05172A114F493DAA8EFFB2666	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\84cdb055-2bf2-4559-9637-934d374fbaf6.tmp **MD5:** C8A68E6E2F21EBE1479FD27EE06FBA3B **SHA256:** FDF6539A9FD777F0F22B16271A0932B0D72B9EDBBE6DBBE4FE9E642D909C1ECD	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Secure Preferences~RF113fe4.TMP **MD5:** 9BC4DCC68994EB09A084CC44ECC6F4E6 **SHA256:** 2D81681CA8E90F7F0FC48382D8AF4336F937EEB1FB49ACFD5249584502D86143	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Secure Preferences **MD5:** C8A68E6E2F21EBE1479FD27EE06FBA3B **SHA256:** FDF6539A9FD777F0F22B16271A0932B0D72B9EDBBE6DBBE4FE9E642D909C1ECD	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\d84adf09-3026-4d02-b3c7-30161456dc08.tmp **MD5:** 90DBBFAF430A82B7BE4F5AACD71C8AF6 **SHA256:** 4CB941176645AAA8F1BC007531F14F94D626C63AE7CB32ECC51F0EF5BB6A0A5A	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity **MD5:** 113CBAB60A2E3A31FF0152F7B19922A6 **SHA256:** 35E7EAFE67371F1B88BAFF04E2F31D8C57814CFABC77ACCABA941E6AA0FD25EB	binary
7684	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\000003.log **MD5:** F49815C37EBBB553EF49CF1F4E42808F **SHA256:** 824AC67E038993AEAE7B77C56899386F9E6C53F6552DF555B7AD67C2CA347A9E	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\2c6db484-626b-40af-a385-aeb712ee4642.tmp **MD5:** 54F6C9CFF7D91E723B2147B978E8FFA2 **SHA256:** 87BC6C4815CB7A6A01362095B29FB2AF8E7FB00CBADFC860559A96F0E13C8B30	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\cf8b6f25-7926-4643-a2f6-4816797660fa.tmp **MD5:** 113CBAB60A2E3A31FF0152F7B19922A6 **SHA256:** 35E7EAFE67371F1B88BAFF04E2F31D8C57814CFABC77ACCABA941E6AA0FD25EB	binary
7516	msedge.exe	C:\Users\admin\AppData\Local\Temp\fd806670-6731-431e-8444-bd7c96bfda5c.tmp **MD5:** FDF8E36CC7970D556A455D24A61FC387 **SHA256:** AA4CB18149973DA9FDEB2F2DD825B17C9CA8C308BF1ACF0129C69665700EAA72	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF11340d.TMP **MD5:** 21F2F7C19D1307E226AA9B173699668F **SHA256:** EBA4881D0D52E08E8D6899BFFC1AB4F59798E9C70D1C2F51875E78D8BAA11C2A	binary
7684	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG **MD5:** E997289723AB624E00743BBD4B4AFB9A **SHA256:** 1CE4D1593AFB465F649F61662ED77AC990E6C224721C418B9C6D746321308311	text
7672	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\000013.log **MD5:** 98230DD045752E47991FD9FA4FC138CC **SHA256:** 32795A4363E30F3FDD39FD94B767ACC059D3C2B46545B9BE03FB1957E5EFBC01	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences **MD5:** 5AF855FBED9D54B4811FB087E3B81C21 **SHA256:** 3FB7F38AE4F1CA87EEBA6DBB37DAEA96865D8BE5C872330005ED3425371D572A	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State~RF11390e.TMP **MD5:** C52DF64918E1FF7FD33C01CBE58342ED **SHA256:** F880EC98D17DA1D0FA9603CBBD969A97C60511264BAFE0A063E2CBABED45085D	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\fdd2fdad-582f-43cf-8d74-ae4e9edb9208.tmp **MD5:** EB7A353D3B85EFD111497EF1BE234B3F **SHA256:** 7283E36028BDCABF6F8457ECAF7F45A2C4E44CA046B17296B33EA789E4B054D1	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF11af86.TMP **MD5:** 90DBBFAF430A82B7BE4F5AACD71C8AF6 **SHA256:** 4CB941176645AAA8F1BC007531F14F94D626C63AE7CB32ECC51F0EF5BB6A0A5A	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\cf2a64a3-9a45-4b98-88a6-eb217a92fc8c.tmp **MD5:** 1F065EC9F81FF65C8CD24BD5EC933F83 **SHA256:** 769EFBCB5BE43FA0D1ED87F00F517D9764661FD6CEDA3AF0D805CB1E780342FB	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\4866e03a-ad1a-4c2d-9bfd-c753c659c721.tmp	binary

		MD5: 5AF855FBED9D54B4811FB087E3B81C21 SHA256: 3FB7F38AE4F1CA87EEBA6DBB37DAEA96865D8BE5C872330005ED3425371D572A	
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RF11b39d.TMP MD5: 113CBAB60A2E3A31FF0152F7B19922A6 SHA256: 35E7EAFE67371F1B88BAFF04E2F31D8C57814CFABC77ACCABA941E6AA0FD25EB	binary
7672	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG MD5: E236692A3DCA21DF1BD7489C4AC9499E SHA256: 6DEBC9F6F528BF80B83C379196BCCB115979EF129AAB34F1080AAB130656A8A6	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1414289814\manifest.fingerprint MD5: 3FB5233616491DF0EC229BA9F42EFDB8 SHA256: 946F3A9E019B0D80F5671DE782F295132341F663F74AEBAD7628F22E528D6D52	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\DualEngine\24f90ab4-c630-4362-9a5b-8357d6ea520f.tmp MD5: 0E3F8C96A0348BB1C7A94E3DA2B68BF0 SHA256: 8232C450F967D7F2F22C54582F0667F4C033AE62E6D450FF8A35C47486249443	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\1d7047f8-a715-4ef0-8edd-0632cef9efee.tmp MD5: 6BDC29C283DBA380E6C1990C14A1F44C SHA256: 2557324BD641893499724472794676D62C310653C9B7EB88D6607F790781895E	binary
1012	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1414289814\manifest.json MD5: AF3A9104CA46F35BB5F6123D89C25966 SHA256: 81BD82AC27612A58BE30A72DD8956B13F883E32FFB54A58076BD6A42B8AFAEEA	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025b MD5: 311F1298863858C8334BD7A8A0E34014 SHA256: 846351F83ED17838A1DE223EAD4E9900D1E127B3243695DAF5A4988E965C44CC	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF11a94d.TMP MD5: 5AF855FBED9D54B4811FB087E3B81C21 SHA256: 3FB7F38AE4F1CA87EEBA6DBB37DAEA96865D8BE5C872330005ED3425371D572A	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_000259 MD5: C8EC290DD651916352F97F3D8270ABD5 SHA256: 2B9C0E305A89862F5BA54D3817CA5407ADBC677D754EE17B6DD8760F82A1F144	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics-spare.pma MD5: — SHA256: —	—
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\569b83f6-dd77-430f-bcda-ca712ac7f025.tmp MD5: 23B4ECD766D17140E01E656143D71384 SHA256: BF3A003D3C8C433A57FE074107EDE7C61B23844E3C99F33D5A80EAF1DE89FAAB	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RF12218a.TMP MD5: 1F065EC9F81FF65C8CD24BD5EC933F83 SHA256: 769EFBCB5BE43FA0D1ED87F00F517D9764661FD6CEDA3AF0D805CB1E780342FB	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\6e529a45-cfb6-4325-81a0-22516a4bc234.tmp MD5: C166F6F7B39AB1946993D64B635E8C22 SHA256: 0BBB89E177C5561187892881656EC22F10A961D9CF1FED240C9BBCB881EFEEDE	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Network Persistent State~RF122b0f.TMP MD5: 54F6C9CFF7D91E723B2147B978E8FFA2 SHA256: 87BC6C4815CB7A6A01362095B29FB2AF8E7FB00CBADFC860559A96F0E13C8B30	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\68771667-5f16-4ca1-b95e-25ead6f03347.tmp MD5: 2410855DDFCAAED7C16ED1AE95A53AD6 SHA256: A3AEC0CA1CFC6628F01CB2CCBC0A1A6CD5B7042A138EAA359DBDD8E602B8A1C7	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF121e4e.TMP MD5: EB7A353D3B85EFD111497EF1BE234B3F SHA256: 7283E36028BDCABF6F8457ECAF7F45A2C4E44CA046B17296B33EA789E4B054D1	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\DualEngine\SiteList-Consumer.json~RF11fd49.TMP MD5: 0E3F8C96A0348BB1C7A94E3DA2B68BF0 SHA256: 8232C450F967D7F2F22C54582F0667F4C033AE62E6D450FF8A35C47486249443	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\DualEngine\SiteList-Consumer.json MD5: 0E3F8C96A0348BB1C7A94E3DA2B68BF0 SHA256: 8232C450F967D7F2F22C54582F0667F4C033AE62E6D450FF8A35C47486249443	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1607842500\manifest.fingerprint MD5: 00766A21BEC3D2DCB091CFE346FB60DD SHA256: B63D4EE5DA0828A109E251CB149F6B0C6968C43714C65C136BE635D631D32E0D	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF12456d.TMP MD5: 2410855DDFCAAED7C16ED1AE95A53AD6 SHA256: A3AEC0CA1CFC6628F01CB2CCBC0A1A6CD5B7042A138EAA359DBDD8E602B8A1C7	binary
8040	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2014965923\manifest.json MD5: 95A16966D590681BA23DEDACEABE0909 SHA256: DC62F38DA3F4D1D52832DCC87BF0A50223681BD2491D18C597864FAD44F2AED6	binary
8004	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1607842500\data.txt MD5: FD8717BAD7CD0F60163E7C2B05210AAA SHA256: D5FACEA6ED705EA08962D52A30EBF38F6D42AEA50A7AF21B103D0388B7DAE34A	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2014965923\manifest.fingerprint MD5: 0C794D6F428E3C6E0D3681B171616F5C SHA256: 54F9CBF488329A02B8D0E5AF3AC758DC1C1C5592B9E9BF1140999ADABD3B3A84	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\1082ac2a-bdec-4c7f-b741-4650b0b4c360.tmp MD5: E2D05749A4DB897F1B3A981A696C03F0 SHA256: 0713A31E9C444CACED388E8605AA54A127B901F33B53ABADEFFFB77624E8674C	binary
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF126c8d.TMP MD5: F86BBFFA2C5C52317999FCEB0593CF92 SHA256: 69C7FC41E992C4E09DF4E9C2FA0D0AD2187F0E5B0B7F649AA3636A14A654F8B0	binary
8084	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_470378815\autofill_bypass_cache_forms.json MD5: 8060C129D08468ED3F3F3D09F13540CE SHA256: B32BFDB89E35959AAF3E61AE58D0BE1DA94A12B6667E281C9567295EFDD92F92	binary
8084	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_470378815\edge_autofill_global_block_list.json MD5: AFB6F8315B244D03B262D28E1C5F6FAE SHA256: A3BCB682DD63C048CD9CA88C49100333651B4F50DE43B60EC681DE5F8208D742	binary
8084	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_470378815\manifest.json MD5: F3EB631411FEA6B5F0F0D369E1236CB3 SHA256: EBBC79D0FCCF58EEAEEE58E3ACBD3B327C06B5B62FC83EF0128804B00A7025D0	text

8004	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1607842500\manifest.json	binary
		MD5: 8C32B9F390FCC4F061885661DBE797BD	**SHA256:** 1431C36E66B4FC53CA74E9B10EA0213245631AD7543FEF183A8DD2720A5B4AB4
6112	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1299136338\ct_config.pb	binary
		MD5: 09B6469DE61DB3473BDFE04951F08529	**SHA256:** 1C435F4448DCF1784637FA9470546D12D7DB2420A11CF8B5D6343439DD401C60
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_470378815\manifest.fingerprint	text
		MD5: 28CB04584014A27ADD5DB903724602D4	**SHA256:** 90182F9357EA3C7F53E5FCF00BA89D1C8FCABCA47024295B18AE6937DCBD42A8
6112	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1299136338\crs.pb	binary
		MD5: 24A3775317D74CEEA8FBA6F0CFBCE562	**SHA256:** 192B206AD6F649F6C8767F6A3B11D9C5354710602BF0AEB4157EEA08D7461EF7
8084	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_470378815\regex_patterns.json	binary
		MD5: B9E8A3075D99D4215D3A778A7BC7222B	**SHA256:** 0F8981B5BB10039061A861AEF0DA28223174056ABE293792039F59DEA84201EC
6112	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1299136338\kp_pinslist.pb	binary
		MD5: 2D8BCB7C4B2DC669429BD40F7048F62A	**SHA256:** 7A0866CDD7BD21B8B08D166EDB3F6ADF8C859B47988B9B3BA3F0EAAFABE10FF2
6112	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1299136338\manifest.json	binary
		MD5: 2C2E90B63E0F7E54FFC271312A3D4490	**SHA256:** 72DBB7D6B647B664EF64B6A14771C2549C979B9C57712F3F712966EDB02D7B2E
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\91a45aed-4d93-4c95-abd5-9240eb86753c.tmp	binary
		MD5: F86BBFFA2C5C52317999FCEB0593CF92	**SHA256:** 69C7FC41E992C4E09DF4E9C2FA0D0AD2187F0E5B0B7F649AA3636A14A654F8B0
8040	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2014965923\typosquatting_list.pb	binary
		MD5: 1E120E110FD933EC69CBAC1BE1646D25	**SHA256:** E2AEC1E11D0EEB89C009D1A60BC8B015461F54956D0097E2C36ECD907843EAC3
4728	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2039243352\manifest.json	binary
		MD5: A30B19BB414D78FFF00FC7855D6ED5FD	**SHA256:** 9811CD3E1FBF80FEB6A52AD2141FC1096165A100C2D5846DD48F9ED612C6FC9F
4728	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2039243352\safety_tips.pb	binary
		MD5: BD6846FFA7F4CF897B5323E4A5DCD551	**SHA256:** 854B7EB22303EC3C920966732BC29F58140A82E1101DFFE2702252AF0F185666
4728	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2039243352\typosquatting_list.pb	binary
		MD5: 17C10DBE88D84B9309E6D151923CE116	**SHA256:** 3AD368C74C9BB5DA4D4750866F16D361B0675A6B6DC4E06E2EDD72488663450E
4728	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2039243352_metadata\verified_contents.json	text
		MD5: EF77CC92636077145827375D5F8D71BC	**SHA256:** 1A8AEE865F808DD81CD980CF2D1B22FF477423723B4B73CB0E491E400A86D105
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_2039243352\manifest.fingerprint	text
		MD5: 10E5B71CE74ECE6A30068113DAA48029	**SHA256:** 24F588CACBF90CDA1C7187B13934E27B6D36B46FCC30DE1E43569854DC9771B4
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\58789fc2-e0ab-4141-9b07-04935159700d.tmp	binary
		MD5: DE7478B2F847D16E6A0C986D891DAECD	**SHA256:** 11C9BD1279C50CF2879D4163DFD6CEC305A3F1B0FFF1424F06A5BC89A58C8C6A
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF121e7d.TMP	binary
		MD5: 9504539EDE9CBF1062E41CE693D42638	**SHA256:** 1B2929C9A95D8B1B3F6F1D49254E8E30B7839647EE97B7D68DE642B40ABDDC91
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1299136338\manifest.fingerprint	text
		MD5: 7D65B590511ABCBE48AD58E49B9A7263	**SHA256:** 71400B86A340E3D8F0048E2190E267DD38374995F47209F6C78E6A2D057BC280
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-af.hyb	binary
		MD5: FFA9DB945F0F0C15B8BBA75A6E064880	**SHA256:** 5487EE44A4CD706D0086522E90C59C76CDF2AC68CE506FD3EAE6054B9220C0CF
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-bn.hyb	binary
		MD5: 8961FDD3DB036DD43002659A4E4A7365	**SHA256:** C2784E33158A807135850F7125A7EAABE472B3CFC7AFB82C74F02DA69EA250FE
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-cs.hyb	binary
		MD5: E8B1509F86508E807D61216614B3DD58	**SHA256:** 97A4755FE9E653A08969F1933E3DB19C712078B227BD5AA6799093ABC5A0EDC3
8084	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_470378815\v1FieldTypes.json	binary
		MD5: 630F694F05BDFB788A9731D59B7A5BFE	**SHA256:** AD6FDEE06AA37E3AF6034AF935F74B58C1933752478026CEECCF47DC506C8779
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-be.hyb	binary
		MD5: 087DE134F3B23A9944AFD711A9667A0B	**SHA256:** 25B7CFA039F82AC92990E1789DE40988D490DB9B613852FB24036B38FF87893C
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-as.hyb	binary
		MD5: 8961FDD3DB036DD43002659A4E4A7365	**SHA256:** C2784E33158A807135850F7125A7EAABE472B3CFC7AFB82C74F02DA69EA250FE
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\38f581ab-3f7f-4aec-b71f-c0f9398e52dc.tmp	binary
		MD5: 9504539EDE9CBF1062E41CE693D42638	**SHA256:** 1B2929C9A95D8B1B3F6F1D49254E8E30B7839647EE97B7D68DE642B40ABDDC91
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-da.hyb	binary
		MD5: D0E160DCA547EDA390D6CC7C4A1F7AC6	**SHA256:** 86FDFC8DB62CDAA11F615DAD3712DA1F4708294E029A4AAD0FC285D4EA16C4BD
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-de-1901.hyb	binary
		MD5: DD9D0A81D897F88F76C1F6D69FB7483E	**SHA256:** 8C5FA4B29519D17593E923BC6A9A284DF7A6D07FAC42F897110B8FB2E0BAEEF5
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-de-1996.hyb	binary
		MD5: E7A9906B316D478B55BF8EBCBBB1D1C5	**SHA256:** D673805547A0228D2F57A5AD551B8760CFCC521F38C49284ED3976E3515BCA49
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-de-ch-1901.hyb	binary
		MD5: C677322984571063 3D3A4D6DD9800FC5	**SHA256:** 8223A912160354E05735522FDB339DC59B353AD5D1E4F4CFA94898DC348E748F
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-el.hyb	binary

		MD5: 746A59E9F9DDA15C0F17C1B72921C85F	**SHA256:** 76AE3454FB0045ADB83094832578AA4749CE4DC694C4EDCF85B419C1E2D9BCD3
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-en-gb.hyb	binary
		MD5: FA3DCB77293A058277CB148A0FF491FA	**SHA256:** AE4B78009D18E849D87458677151EE3AAD1608AD72EC050DFD2421D22E7D031F
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-en-us.hyb	binary
		MD5: B2693233D14890C81D322BEC948549E7	**SHA256:** 03727CD6F4AA71B203C4C74CA6987AC7D87F13037337AC6F4B6996C2A0DC5F8C
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-et.hyb	binary
		MD5: 2AE42AB807286F6EC0FF1876D9536B0B	**SHA256:** 10079C66014DD2E6ABFEF5A018E6553FD5A036AFB96BD2A235440A188F88B15E
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF1294a7.TMP	binary
		MD5: E2D05749A4DB897F1B3A981A696C03F0	**SHA256:** 0713A31E9C444CACED388E8605AA54A127B901F33B53ABADEFFFB77624E8674C
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-bg.hyb	binary
		MD5: E8A4F8F5238F9A0FF6968AD8DBA2755F	**SHA256:** 7593F0395081E3EEB2D8516D10746608AFD826CFFD4E7E37D53936993D200A13
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-eu.hyb	binary
		MD5: E90EA97070CFCFA795FBD807AC300D34	**SHA256:** E2778A4FC7B8F064A32B6A44BC29F10E264D9D6214B8EDB8EBD1F5F6D68E2EB2
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-fr.hyb	binary
		MD5: 092E0A95D6DADA26CA56D2ED558749A3	**SHA256:** 00BD8B2D398D77575DA2BFBBC5EC641AAD7F2A87D4A31186EC169E85A27DE5B7
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-ga.hyb	binary
		MD5: 768032A419E0AE3BD870D591E2173715	**SHA256:** 1E3043F395BFB2A4C43D0480BA2F168ED622881CC3482359CA6E99821E983BE8
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-gl.hyb	binary
		MD5: 1B08FB098D29C30488B8FC3F19DCF8B9	**SHA256:** 89D98EFF14E2CF1C2314EFDF392339E62D7E786F100202A7377BF7B22095A0C5
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-gu.hyb	binary
		MD5: F6DC4E0FB974869D3D9457C582A38690	**SHA256:** AF0EDB67C2219B803C3EB6C1DEE6F2D41A3FE00468A9DA8BE8EF5056D701ABF3
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-es.hyb	binary
		MD5: F6BD0377237FCA3C4B7C6A6CB244298B	**SHA256:** 137461792537A2E56A6475E81E2B9AD7A2BDABF1F4738FAE186DCA3022357349
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-cy.hyb	binary
		MD5: B0F32ED7B4B8A068A962D820627B7229	**SHA256:** 4D0569FE2F4B41B3164CF610310E1D996FD2C553CC39DE6062E50F4E033CC207
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-cu.hyb	binary
		MD5: B4E5921B1DF85BA9F2EBE6CE578915F6	**SHA256:** 2BAEE19D5024FF87DCF3A1B9D0DA1B3AC5A1E506ADEEAD3B96A4DE5395D0290E
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-hi.hyb	binary
		MD5: 0807CF29FC4C5D7D87C1689EB2E0BAAA	**SHA256:** F4DF224D459FD111698DD5A13613C5BBF0ED11F04278D60230D028010EAC0C42
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-hr.hyb	binary
		MD5: 1864E47E724BB7F9C052A2840EEE21D9	**SHA256:** D5F066A5657F1D7C39D053956DF204B7926F40D2FE4F69573AF09D909066E26C
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-hu.hyb	binary
		MD5: 37B1F197E8DFBAFDAC4597EDCF673E63	**SHA256:** 8B3A16268CC932B226C17FF405B3CFB6EB38A9511A2043D653DC03729EFCEAC1
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-hy.hyb	binary
		MD5: 70EA4451C3A26FD7197A3D2188BE4152	**SHA256:** 9B34DFCA85CB27546829F104F137757EFB274934C1E9D4991F55AD564962A76A
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-it.hyb	binary
		MD5: A4D5EC24D4C5EE745CDCDC019018074F	**SHA256:** F9C027D7FD44B01CD5E1CDF802E20C63560673098AF18BEA0930BA9AF334E0F7
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-ka.hyb	binary
		MD5: AA6C771083158380B2631F01E3F64F20	**SHA256:** 2472271C7955C67E9FDB86D0CD3C5D88F5E598DA4F44B6741284B2BBCB2E4D52
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-kn.hyb	binary
		MD5: D986AC2E7C75CF3EF929A7A269AE0D5A	**SHA256:** 2B999D0A152F804601AA8F38FF0D3A6E5949977BF1DAA76FA888ACAE21526287
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-la.hyb	binary
		MD5: 9AAA47272099A013A4389BC314B7D2ED	**SHA256:** FD4B6F36135CD3B932E350EC2017DFD89D2E36AC226F54E4C8F2E4BC6DB0593D
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-lt.hyb	binary
		MD5: 970C2671EAC4FFF6D840DC122E43B7C6	**SHA256:** 6FE2DA26A96834FB9AECBE586D40F728DF0EF676A4F235450054E66841B9E2CA
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-lv.hyb	binary
		MD5: 05DFDB7F1EE5744573CCD62AE565B2C7	**SHA256:** 65962CCB5055E4C693E5AC493D6AFFDC810EC168EB2942F5705B7F4E464F9993
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-mn-cyrl.hyb	binary
		MD5: 07CDA8332B62726883B29290CA35FC89	**SHA256:** 0D2731F16AA2C90FAEC8E63260358CBCCEDE403FAF95E3AF8C66BC2DB0729CA0
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-mr.hyb	binary
		MD5: 0807CF29FC4C5D7D87C1689EB2E0BAAA	**SHA256:** F4DF224D459FD111698DD5A13613C5BBF0ED11F04278D60230D028010EAC0C42
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-mul-ethi.hyb	binary
		MD5: B42317960E5DA868A8120CB79A440ABF	**SHA256:** F2FAC1BD069FFE5CD1112D94CC31137ED38A1B161093ECD74C9C1688428B688B
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-nb.hyb	binary
		MD5: 677EDD1A17D50F0BD11783F58725D0E7	**SHA256:** C2771FBB1BFFF7DB5E267DC7A4505A9675C6B98CFE7A8F7AE5686D7A5A2B3DD0
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-nl.hyb	binary
		MD5: D3BB05944DE3D0D7186E7E9383805E2C	**SHA256:** 5EBDE398944B461CF940F0520C5A49C0882B6F36F9AC5CDA0538C8C8B44FB7CA

7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-nn.hyb **MD5:** F2D8FE158D5361FC1D4B794A7255835A **SHA256:** 5BCBB58EAF65F13F6D039244D942F37C127344E3A0A2E6C32D08236945132809	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-ml.hyb **MD5:** 84A0A36EA2C5B3209A3CD40D1043230F **SHA256:** 90572DB8F49B01EC6A102732CDF14FC3F07D363CBE0D261103E583043164E888	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-pt.hyb **MD5:** 564FF32DED64C6BFC693F2758A53D68E **SHA256:** F6FBF1BCB260CC86256FC494F388F7B27D10865FBF8F61517DEE25AF4D58D6E8	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-ru.hyb **MD5:** 4D132AB42E0C8ABD3BA93D8B34BDBEB3 **SHA256:** 336CE2048FFD31B7BCAF435E53BADFAF0579E405042D49ADBC0823F6BE5F9614	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-sk.hyb **MD5:** CEA295E8B4B99F95738727905A9184E2 **SHA256:** 138C5990961DA21993653F54A413DDACB8921D6D70B892B7CA154D6E8AD2028C	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-sl.hyb **MD5:** A21358DD4506643486F72F7D80D60A5B **SHA256:** AD746C68562603AC3B15E89DA03C76E081C08E7D9C8D4C9F64763E53D696C77C	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-sq.hyb **MD5:** A22D0F39CD83F3A8E251F95C5B12DD31 **SHA256:** BC29C9401CE952414CBAEBC5C8EE1D27C1706C6F77807B5FF713E2124438B3CA	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-sv.hyb **MD5:** 892598DC59CE71E68ED337ED9FF3ABC1 **SHA256:** 56642AA5A37625FF9D034761D16B034D4BA5BE74090CBD825956BBCE2775ECD1	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-ta.hyb **MD5:** AB2F6F9696FC7D699356244725E7C778 **SHA256:** 40FDA94856A86F065DE8BAA6184EA63DCDB011EE4CA498A7C1FEE44C99314C67	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-te.hyb **MD5:** BF9DF63B3C97DE3BFF99E24EE4BC5F2E **SHA256:** 516FA9654FA3AEAAB480D40EAF6AD78FC039086BD8EDC144BE3D59525EDCAC29	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-tk.hyb **MD5:** ED60185B6F455B6F8ED27EAEB73334A9 **SHA256:** 77FDAED29BD842AAA976AB7EF81B617A15C0A2D1EBD1161C1BF26B79A108B5CD	binary
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\shopping.js **MD5:** — **SHA256:** —	—
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-uk.hyb **MD5:** 0EC028755F0CD9EBBA41FB7273DE8BAF **SHA256:** 1C626ABE40D43F6D56A01B5B40305D7C7D6481F616EAC00A3F3AAAACA8388786	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-or.hyb **MD5:** 7E265A294303F69AA66C243F5F474463 **SHA256:** 4E9CD302BAFFC4EA3E9652327EA24072EBF37B5C4FC0719292BDAC10AAAD665B	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-und-ethi.hyb **MD5:** 4AA9B2C0C9CCDE5140D01DC6502242BB **SHA256:** 1DE83CB787DFAF53FB7E6E8DB3AAE5008AD24EBDD28BE02031306EA9E9F3E285	binary
5332	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00025a **MD5:** D17B5A55EC9D8608C1D2B531CCB6DE88 **SHA256:** DC2A3600C7CDFAEA40DB03757D6915D67518215DB51397C8A5BB3F132AE89A49	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\manifest.json **MD5:** 2617C38BED67A4190FC499142B6F2867 **SHA256:** D571EF33B0E707571F10BB37B99A607D6F43AFE33F53D15B4395B16EF3FDA665	binary
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681_metadata\verified_contents.json **MD5:** 117D173E82B282DECA740475E35C8ECD **SHA256:** 65491B21947D60C87C6358DCF69DF9ACA2B99E8F3B611BD3D559699BBC25000B	text
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\manifest.fingerprint **MD5:** 1D09A9A5E62B846125CD7B929CCCBE44 **SHA256:** 1703E4E777B285ABA435E71256890A5FE92D24CB01E0EEFD03BADDCA228EEE2F	text
7724	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_1759849681\hyph-pa.hyb **MD5:** 0F27E5BCCC1CD9DDF3EAC020DA27DA57 **SHA256:** 470329D28FAA484F945D78FFEFB176DCB6F2032C753E25BC014106AD24B2C68A	binary
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\auto_open_controller.js **MD5:** 3237F9875553958FCD58B80388DEE28B **SHA256:** D4962432626228AAFCB0006C8384AA0FEF0169CB6158623F2821617875A9217D	binary
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\edge_checkout_page_validator.js **MD5:** 63943F17C56D9DEF79CBD0DE073A2EFF **SHA256:** F296D1A16546F8A22153BC031FB44C4447123D0B70906FA3B4873DD2DEF6D714	binary
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\edge_confirmation_page_validator.js **MD5:** F2FFE67863CC3BDCE99DFE09798CE415 **SHA256:** 4B58B498794FB539200E5A85F44AA6472436C4EEBDF1E2A61E1077A18B601A4F	binary
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\edge_driver.js **MD5:** 1A084415F501751C26B5B5EFCAD15D1B **SHA256:** 5AAC285971BCC66DBD1D2850DFEF2E2F9CD6E9D89F8E4D41C1703AAFABD8D932	binary
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\edge_tracking_page_validator.js **MD5:** E900A0187F65069DE0A5012363133873 **SHA256:** 551FA9D0133F9DB8CEA712CD5F08B9D2ECFC417C1C09EEE3D5E975F378F72E70	binary
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\manifest.json **MD5:** 2F8236D78F767F9986F0F418F697C9D8 **SHA256:** 4BEEAC63D5170854FECC138D006795B0C1CEEF32A672404DFD8D41464EA2C780	text
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\product_page.js **MD5:** 5F069C1BC9A83DBB74B180944CBCEA61 **SHA256:** 171D3E1F1C54043B3F1D1679642076446F8C5EDE30715DF9D4672488FC5E112E	binary
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\shopping.html **MD5:** 0E8308D5832852AD3C299F0C63EEA163 **SHA256:** 4A07676F7B8F79D9DB68E385485DAA5912CBC46CBF1BCC003F2CAACFD1132E35	html
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\shoppingfre.js	binary

		MD5: 16D1409BAB41547D1F6BEB8109C005EC	**SHA256:** 053494C396955ABF183164C886251651B0F55CCEFD85EC9F3BBDFB763CCA53A9
6640	msedge.exe	C:\Users\admin\AppData\Local\D3DSCache\f4d41c5d09ae781\F4EB2D6C-ED2B-4BDD-AD9D-F913287E6768.lock	text
		MD5: F49655F856ACB8884CC0ACE29216F511	**SHA256:** 7852FCE59C67DDF1D6B8B997EAA1ADFAC004A9F3A91C37295DE9223674011FBA
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\113d4d09-8a8f-4998-a427-3577590b2a96.tmp	binary
		MD5: 34DF459597B5E8633CFD32972D127F82	**SHA256:** 42EC1EE5BC7A50ACF7B5D1F9720B7DF0FA17EBC7B8F9885A4EC02067F8ACBEEE
1328	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\manifest.fingerprint	text
		MD5: B4DC7755EF86DE6FAB3122E533920752	**SHA256:** 1E3CD0F418CA2A7C94735E8E6AAC3DFFF469758F064FF9F91C0669D597C8398B
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\shopping_iframe_driver.js	binary
		MD5: 893BB91220344CE92E1B46C4B0C3A548	**SHA256:** 9E5DF6E98F0CFB46AEC92421B0A2B62F95C4F55F94AB5C198B374B121885CE91
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF12d847.TMP	binary
		MD5: DE7478B2F847D16E6A0C986D891DAECD	**SHA256:** 11C9BD1279C50CF2879D4163DFD6CEC305A3F1B0FFF1424F06A5BC89A58C8C6A
7576	msedge.exe	C:\Users\admin\AppData\Local\Temp\chrome_Unpacker_BeginUnzipping1328_594967816\shopping_fre.html	html
		MD5: 455B071F9EB0A250CF1FB1DB939A662E	**SHA256:** CB3C58B8099A90347BDC1A8F1B3D9FF7A011E63AFA5D66A40BD4FB00FF14D91C
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\95c626e9-073b-4020-b867-375784f6eae0.tmp	binary
		MD5: 07FEBC12FDA0377163F995CF1A3AA306	**SHA256:** 124CB80470ECFCA547B55E49FBAC8643AD388F94E92E5BDD5B7D09151A601CA8
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF130a73.TMP	binary
		MD5: 23B4ECD766D17140E01E656143D71384	**SHA256:** BF3A003D3C8C433A57FE074107EDE7C61B23844E3C99F33D5A80EAF1DE89FAAB
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF130b4e.TMP	binary
		MD5: 34DF459597B5E8633CFD32972D127F82	**SHA256:** 42EC1EE5BC7A50ACF7B5D1F9720B7DF0FA17EBC7B8F9885A4EC02067F8ACBEEE
1328	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\ed7c9d6b-4b52-459a-8324-7911a9b3ff87.tmp	binary
		MD5: 6D289363EA62FA77F04862E2F7C2C074	**SHA256:** E2770CA2033746E5B0709C49FA3C4741390EC6A69BE2F14CC718B50A7D595D4D

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
62	56	50	1

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
–	–	GET	401	13.107.6.158:443	https://business.bing.com/api/v1/user/token/microsoftgraph?&clienttype=edge-omnibox	unknown	–	–	–
–	–	GET	304	13.107.21.239:443	https://edge.microsoft.com/abusiveadblocking/api/v1/blocklist	unknown	–	–	–
–	–	GET	200	13.107.246.44:443	https://edgeassetservice.azureedge.net/assets/domains_config_gz/3.0.7/asset?assetgroup=EntityExtractionDomainsConfig	unknown	–	–	–
–	–	GET	200	13.107.42.16:443	https://config.edge.skype.com/config/v1/Edge/122.0.2365.59?clientId=4489578223053569932&agents=EdgeFirstRun%2CEdgeFirstRunConfig&osname=win&client=edge&channel=stable&scpfre=0&osarch=x86_64&osver=10.0.19045&wu=1&devicefamily=desktop&uma=0&sessionid=44&mngd=0&installdate=1661339457&edu=0&bphint=2&soobedate=1504771245&fg=1	unknown	binary	768 b	whitelisted
–	–	GET	200	13.107.253.44:443	https://edge-mobile-static.azureedge.net/eccp/get?settenant=edge-config&setplatform=win&setmkt=en-US&setchannel=stable	unknown	binary	14.4 Kb	whitelisted
–	–	GET	401	13.107.6.158:443	https://business.bing.com/work/api/v2/tenant/my/settingswithflights?&clienttype=edge-omnibox	unknown	binary	589 b	whitelisted
–	–	GET	200	13.107.21.239:443	https://edge.microsoft.com/serviceexperimentation/v3/?osname=win&channel=stable&osver=10.0.19045&devicefamily=desktop&installdate=1661339457&clientversion=122.0.2365.59&experimentationmode=2&scpguard=0&scpfull=0&scpver=0	unknown	binary	689 b	whitelisted
–	–	GET	404	78.46.117.95:443	https://freedesktopsoft.com/butterflyondesktoplike.html	unknown	html	266 b	malicious
–	–	OPTIONS	503	2.16.10.175:443	https://bzib.nelreports.net/api/report?cat=bingbusiness	unknown	html	280 b	whitelisted
–	–	GET	200	13.107.42.16:443	https://config.edge.skype.com/config/v1/Edge/122.0.2365.59?clientId=4489578223053569932&agents=Edge%2CEdgeConfig%2CEdgeServices%2CEdgeFirstRun%2CEdgeFirstRunConfig&osname=win&client=edge&channel=stable&scpfre=0&osarch=x86_64&osver=10.0.19045&wu=1&devicefamily=desktop&uma=0&sessionid=44&mngd=0&installdate=1661339457&edu=0&bphint=2&soobedate=1504771245&fg=1	unknown	binary	9.65 Kb	whitelisted
–	–	GET	404	78.46.117.95:443	https://freedesktopsoft.com/favicon.ico	unknown	html	266 b	malicious
–	–	GET	200	13.107.21.239:443	https://edge.microsoft.com/extensionwebstorebase/v1/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=edgecrx&prodchannel=&prodversion=122.0.2365.59&lang=en-	unknown	xml	413 b	whitelisted

					US&acceptformat=crx3,puff&x=id%3Djmjflgjpcpepeafmmgdpfkogkghcpiha%26v%3D1.2.1%26installedby%3Dother%26uc%26ping%3Dr%253D230%2526e%253D1				
–	–	POST	200	142.250.186.99:443	https://update.googleapis.com/service/update2/json?cup2key=13:eu7MU1vq9XcENV8MJngkOFyxQZPau8WpdMyJhZzVyI0&cup2hreq=ccd8094a90e47481273f90731581445d970920bca1b17c4789740f0db4da0835	unknown	text	889 b	whitelisted
–	–	GET	200	104.126.37.177:443	https://edgeservices.bing.com/edgesvc/userstatus	unknown	binary	381 b	whitelisted
–	–	GET	200	104.126.37.137:443	https://www.bing.com/bloomfilterfiles/ExpandedDomainsFilterGlobal.json	unknown	binary	652 Kb	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/fb6dd03b-99d7-4cc8-a878-91c8e655c2d3?P1=1741792158&P2=404&P3=2&P4=aQZbriZca9jglWDVVNtAPL%2fla5DUea1LayAoNFAdGhQLRmkCl%2ftSCCCmsRrA555eexblnLEMj74dhqenWgzUQw%3d%3d	unknown	–	–	whitelisted
–	–	GET	200	204.79.197.239:443	https://edge.microsoft.com/entityextractiontemplates/api/v1/assets/find-assets?name=domains_config_gz&version=3.*.*&channel=stable&key=d414dd4f9db345fa8003e32adc81b362	unknown	text	265 b	whitelisted
–	–	GET	200	216.58.206.65:443	https://clients2.googleusercontent.com/crx/blobs/ASuc5ohcoRYyASTWkAI21BvR0f-Aos7pzgW3GtD8ImYoX-O9Pl77join3GT-5wpD1vT_nG6xpJ0eds7JOZacv0OYNfBAee3mKSnMDx3-YDnz3J7UxfHM_wfhsyHz9Z8rajAAxlKa5T9frrLIN0KHGfJRu7Y7NseNtZ_M/GHBMNNJOOEKPMOECNNNILNNBDLOLHKHI_1_89_1_0.crx	unknown	binary	150 Kb	whitelisted
–	–	GET	302	2.23.246.101:443	https://go.microsoft.com/fwlink/?linkid=2133855&bucket=15	unknown	–	–	–
1600	svchost.exe	HEAD	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/fb6dd03b-99d7-4cc8-a878-91c8e655c2d3?P1=1741792158&P2=404&P3=2&P4=aQZbriZca9jglWDVVNtAPL%2fla5DUea1LayAoNFAdGhQLRmkCl%2ftSCCCmsRrA555eexblnLEMj74dhqenWgzUQw%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/fb6dd03b-99d7-4cc8-a878-91c8e655c2d3?P1=1741792158&P2=404&P3=2&P4=aQZbriZca9jglWDVVNtAPL%2fla5DUea1LayAoNFAdGhQLRmkCl%2ftSCCCmsRrA555eexblnLEMj74dhqenWgzUQw%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	HEAD	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/f28d972a-574d-41b9-8559-4ab486e8a4f0?P1=1741792161&P2=404&P3=2&P4=Kb59bO7cZZUASPRY0Th9CKyebFZLWc0VRId9tpLlCaAP1VYv8GETcybQFPK8YEuYk6oIwSIFGg7pKz7s30BWYg%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/f28d972a-574d-41b9-8559-4ab486e8a4f0?P1=1741792161&P2=404&P3=2&P4=Kb59bO7cZZUASPRY0Th9CKyebFZLWc0VRId9tpLlCaAP1VYv8GETcybQFPK8YEuYk6oIwSIFGg7pKz7s30BWYg%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/f28d972a-574d-41b9-8559-4ab486e8a4f0?P1=1741792161&P2=404&P3=2&P4=Kb59bO7cZZUASPRY0Th9CKyebFZLWc0VRId9tpLlCaAP1VYv8GETcybQFPK8YEuYk6oIwSIFGg7pKz7s30BWYg%3d%3d	unknown	–	–	whitelisted
–	–	GET	200	13.107.246.44:443	https://xpaywalletcdn.azureedge.net/mswallet/ExpressCheckout/v2/GetEligibleSites?version=0&type=commonConfig&IsStable=false	unknown	binary	481 b	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/f28d972a-574d-41b9-8559-4ab486e8a4f0?P1=1741792161&P2=404&P3=2&P4=Kb59bO7cZZUASPRY0Th9CKyebFZLWc0VRId9tpLlCaAP1VYv8GETcybQFPK8YEuYk6oIwSIFGg7pKz7s30BWYg%3d%3d	unknown	–	–	whitelisted
–	–	GET	200	13.107.246.44:443	https://edge-consumer-static.azureedge.net/mouse-gesture/config.json	unknown	binary	101 b	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/f28d972a-574d-41b9-8559-4ab486e8a4f0?P1=1741792161&P2=404&P3=2&P4=Kb59bO7cZZUASPRY0Th9CKyebFZLWc0VRId9tpLlCaAP1VYv8GETcybQFPK8YEuYk6oIwSIFGg7pKz7s30BWYg%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/f28d972a-574d-41b9-8559-4ab486e8a4f0?P1=1741792161&P2=404&P3=2&P4=Kb59bO7cZZUASPRY0Th9CKyebFZLWc0VRId9tpLlCaAP1VYv8GETcybQFPK8YEuYk6oIwSIFGg7pKz7s30BWYg%3d%3d	unknown	–	–	whitelisted
–	–	GET	200	204.79.197.239:443	https://edge.microsoft.com/entityextractiontemplates/api/v1/assets/find-assets?name=arbitration_priority_list&version=9.*.*&channel=stable&key=d414dd4f9db345fa8003e32adc81b362	unknown	text	271 b	whitelisted
–	–	GET	200	13.107.21.239:443	https://edge.microsoft.com/entityextractiontemplates/api/v1/assets/find-assets?name=edge_hub_apps_manifest_gz&version=4.10.*&channel=stable&key=d414dd4f9db345fa8003e32adc81b362	unknown	text	266 b	whitelisted
–	–	GET	200	13.107.42.16:443	https://config.edge.skype.com/config/v1/Edge/122.0.2365.59?clientId=4489578223053569932&agents=EdgeRuntime%2CEdgeRuntimeConfig%2CEdgeDomainActions&osname=win&client=edge&channel=stable&scpfre=0&osarch=x86_64&osver=10.0.19045&wu=1&devicefamily=desktop&uma=0&sessionid=44&mngd=0&installdate=1661339457&edu=0&bphint=2&sobedate=1504771245&fg=1	unknown	binary	43.3 Kb	whitelisted
1600	svchost.exe	HEAD	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/07ef1e64-cfc1-48b7-9b0e-09c976e9cf12?P1=1741768354&P2=404&P3=2&P4=M%2ffGx56Tf5lmuHMz	unknown	–	–	whitelisted

					l%2bQs0MFrixav%2bcNDWjrXz2YMAg3jW1QiG0wauH8W1D				
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/07ef1e64-cfc1-48b7-9b0e-09c976e9cf12?P1=1741768354&P2=404&P3=2&P4=M%2ffGx56Tf5lmuHMzl%2bQs0MFrixav%2bcNDWjrXz2YMAg3jW1QiG0wauH8W1DguhwxM8vzGlVevdw2qaECw9EeTJw%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/07ef1e64-cfc1-48b7-9b0e-09c976e9cf12?P1=1741768354&P2=404&P3=2&P4=M%2ffGx56Tf5lmuHMzl%2bQs0MFrixav%2bcNDWjrXz2YMAg3jW1QiG0wauH8W1DguhwxM8vzGlVevdw2qaECw9EeTJw%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	HEAD	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/e97d85e8-2e6f-4c6c-8a9a-1d07973733be?P1=1741581877&P2=404&P3=2&P4=dqrxirOP%2fMAzZusid6bBVv7x2Xax7ajsm9JaVRlD3w0TjeVSVG07d45WPqP9uEpHhcqBGZE8H9U9yKg8xord8w%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/e97d85e8-2e6f-4c6c-8a9a-1d07973733be?P1=1741581877&P2=404&P3=2&P4=dqrxirOP%2fMAzZusid6bBVv7x2Xax7ajsm9JaVRlD3w0TjeVSVG07d45WPqP9uEpHhcqBGZE8H9U9yKg8xord8w%3d%3d	unknown	–	–	whitelisted
–	–	GET	200	13.107.246.44:443	https://xpaywalletcdn.azureedge.net/mswallet/ExpressCheckout/v2/GetEligibleSites?version=0&type=topSite&IsStable=false	unknown	binary	497 b	whitelisted
–	–	GET	404	78.46.117.95:443	https://freedesktopsoft.com/butterflyondesktoplike.html	unknown	html	266 b	malicious
–	–	GET	200	13.107.246.44:443	https://xpaywalletcdn.azureedge.net/mswallet/ExpressCheckout/v2/GetEligibleSites?version=0&type=dafSite&IsStable=false	unknown	binary	332 Kb	whitelisted
–	–	POST	200	13.107.21.239:443	https://edge.microsoft.com/componentupdater/api/v1/update?cup2key=7:CtbbQkPEs6yRXl2wwxTWPSZ1LW8l8GwZp0QPqRYTm-I&cup2hreq=d1d04cb1ec22ae56984ee9f988d7e466614c7365244fecaf04cd4b651da8ff63	unknown	text	17.5 Kb	whitelisted
–	–	GET	200	13.107.21.239:443	https://edge.microsoft.com/neededge/v1?bucket=15	unknown	xml	741 Kb	whitelisted
–	–	OPTIONS	503	2.16.10.175:443	https://bzib.nelreports.net/api/report?cat=bingbusiness	unknown	html	280 b	whitelisted
–	–	POST	500	40.91.76.224:443	https://activation-v2.sls.microsoft.com/SLActivateProduct/SLActivateProduct.asmx?configextension=Retail	unknown	xml	512 b	whitelisted
1600	svchost.exe	HEAD	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/6ca9004c-2afd-40c0-a9b1-4fec460952e5?P1=1741792160&P2=404&P3=2&P4=PaUVOEqUm0apcJdUW2QeZ7J7YcWzGIaisuBdjBe3smRT5Px5zjtSBZcc4tPFvMkgJNe%2bNMDDBPQz8LzG9IdYEg%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/6ca9004c-2afd-40c0-a9b1-4fec460952e5?P1=1741792160&P2=404&P3=2&P4=PaUVOEqUm0apcJdUW2QeZ7J7YcWzGIaisuBdjBe3smRT5Px5zjtSBZcc4tPFvMkgJNe%2bNMDDBPQz8LzG9IdYEg%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/5cbc98ff-b69b-4fda-ad94-17ec2f9cf48b?P1=1741788558&P2=404&P3=2&P4=LonBRFULbRdz2Q%2fgalW4VHsbJSGlSNp7wxjGE2x0rVoN6Guye7iSKTU%2b%2b7NHLcrspQgiKDhYDz6FUwW0snSjIQ%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	HEAD	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/68591036-2289-4858-9f7f-9149e89c8a08?P1=1741792158&P2=404&P3=2&P4=ZxVdq7ALpZ7Zee337dDAyXvjgwqda5PChzpmhsLB0bV2BnC8S3QG92izFPWawQG4OhxnTLV8W43581Nu6ixNEA%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/68591036-2289-4858-9f7f-9149e89c8a08?P1=1741792158&P2=404&P3=2&P4=ZxVdq7ALpZ7Zee337dDAyXvjgwqda5PChzpmhsLB0bV2BnC8S3QG92izFPWawQG4OhxnTLV8W43581Nu6ixNEA%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/370be913-fe5a-455b-af7f-6ca894b905e8?P1=1741309043&P2=404&P3=2&P4=k8jwU0MsNB9OOrCK9V4N77sDxoRfgzQlldR9H0UCdHI7kyIQyzsNW00eWllBPLIfa4J3QOPzZ4WPYOpQYy365w%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	HEAD	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/5cbc98ff-b69b-4fda-ad94-17ec2f9cf48b?P1=1741788558&P2=404&P3=2&P4=LonBRFULbRdz2Q%2fgalW4VHsbJSGlSNp7wxjGE2x0rVoN6Guye7iSKTU%2b%2b7NHLcrspQgiKDhYDz6FUwW0snSjIQ%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	HEAD	200	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/370be913-fe5a-455b-af7f-6ca894b905e8?P1=1741309043&P2=404&P3=2&P4=k8jwU0MsNB9OOrCK9V4N77sDxoRfgzQlldR9H0UCdHI7kyIQyzsNW00eWllBPLIfa4J3QOPzZ4WPYOpQYy365w%3d%3d	unknown	–	–	whitelisted
1600	svchost.exe	GET	206	199.232.214.172:80	http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/370be913-fe5a-455b-af7f-6ca894b905e8?P1=1741309043&P2=404&P3=2&P4=k8jwU0MsNB9OOrCK9V4N77sDxoRfgzQlldR9H0UCdHI7kyIQyzsNW00eWllBPLIfa4J3QOPzZ4WPYOpQYy365w%3d%3d	unknown	–	–	whitelisted
–	–	POST	200	204.79.197.239:443	https://edge.microsoft.com/componentupdater/api/v1/update	unknown	text	214 b	whitelisted
–	–	POST	200	13.107.21.239:443	https://edge.microsoft.com/componentupdater/api/v1/update	unknown	text	213 b	whitelisted

–	–	POST	200	204.79.197.239:443	https://edge.microsoft.com/componentupdater/api/v1/update	unknown	–	–	whitelisted
–	–	POST	500	40.91.76.224:443	https://activation-v2.sls.microsoft.com/SLActivateProduct/SLActivateProduct.asmx?configextension=Retail	unknown	xml	512 b	whitelisted
–	–	POST	200	204.79.197.239:443	https://edge.microsoft.com/componentupdater/api/v1/update	unknown	text	214 b	whitelisted
–	–	POST	200	13.107.21.239:443	https://edge.microsoft.com/componentupdater/api/v1/update	unknown	text	215 b	whitelisted
–	–	POST	200	13.107.21.239:443	https://edge.microsoft.com/componentupdater/api/v1/update	unknown	text	214 b	whitelisted
–	–	POST	200	204.79.197.239:443	https://edge.microsoft.com/componentupdater/api/v1/update	unknown	text	213 b	whitelisted
–	–	POST	200	204.79.197.239:443	https://edge.microsoft.com/componentupdater/api/v1/update	unknown	text	214 b	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
–	–	192.168.100.255:137	–	–	–	whitelisted
2104	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
–	–	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
2104	svchost.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5332	msedge.exe	13.107.42.16:443	config.edge.skype.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
1328	msedge.exe	239.255.255.250:1900	–	–	–	whitelisted
5332	msedge.exe	13.107.21.239:443	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
5332	msedge.exe	13.107.246.44:443	edge-mobile-static.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
5332	msedge.exe	78.46.117.95:80	freedesktopsoft.com	Hetzner Online GmbH	DE	malicious
5332	msedge.exe	13.107.6.158:443	business.bing.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
5332	msedge.exe	78.46.117.95:443	freedesktopsoft.com	Hetzner Online GmbH	DE	malicious
5332	msedge.exe	2.16.10.182:443	bzib.nelreports.net	Akamai International B.V.	AT	whitelisted
5332	msedge.exe	142.250.186.99:443	update.googleapis.com	GOOGLE	US	whitelisted
1328	msedge.exe	224.0.0.251:5353	–	–	–	unknown
5332	msedge.exe	104.126.37.177:443	edgeservices.bing.com	Akamai International B.V.	DE	whitelisted
5332	msedge.exe	216.58.206.65:443	clients2.googleusercontent.com	GOOGLE	US	whitelisted
5332	msedge.exe	13.107.246.60:443	edge-consumer-static.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
4224	slui.exe	40.91.76.224:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
5332	msedge.exe	2.19.246.123:443	go.microsoft.com	AKAMAI-AS	DE	whitelisted
3812	svchost.exe	239.255.255.250:1900	–	–	–	whitelisted
5332	msedge.exe	104.124.11.32:443	bzib.nelreports.net	Akamai International B.V.	DE	whitelisted
1600	svchost.exe	199.232.214.172:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	FASTLY	US	whitelisted
5332	msedge.exe	2.23.227.215:443	www.bing.com	–	–	whitelisted
1348	slui.exe	20.83.72.98:443	activation-v2.sls.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
5332	msedge.exe	2.23.227.208:443	www.bing.com	–	–	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	40.127.240.158 51.124.78.146	whitelisted
google.com	216.58.212.142	whitelisted
config.edge.skype.com	13.107.42.16	whitelisted

freedesktopsoft.com	78.46.117.95	malicious
edge.microsoft.com	13.107.21.239 204.79.197.239	whitelisted
edge-mobile-static.azureedge.net	13.107.246.44	whitelisted
business.bing.com	13.107.6.158	whitelisted
bzib.nelreports.net	2.16.10.182 2.16.10.175 104.124.11.32 104.124.11.19	whitelisted
update.googleapis.com	142.250.186.99	whitelisted
edgeservices.bing.com	104.126.37.177 104.126.37.176 104.126.37.123 104.126.37.179 104.126.37.171 104.126.37.139 104.126.37.131 104.126.37.161 104.126.37.130	whitelisted
clients2.googleusercontent.com	216.58.206.65	whitelisted
edgeassetservice.azureedge.net	13.107.246.44	whitelisted
www.bing.com	104.126.37.177 104.126.37.176 104.126.37.123 104.126.37.179 104.126.37.171 104.126.37.139 104.126.37.131 104.126.37.161 104.126.37.130 2.23.227.215 2.23.227.208	whitelisted
edge-consumer-static.azureedge.net	13.107.246.60	whitelisted
xpaywalletcdn.azureedge.net	13.107.246.44	whitelisted
activation-v2.sls.microsoft.com	40.91.76.224 20.83.72.98	whitelisted
go.microsoft.com	2.19.246.123	whitelisted
msedge.b.tlu.dl.delivery.mp.microsoft.com	199.232.214.172 199.232.210.172	whitelisted

Threats

PID	Process	Class	Message
–	–	Potentially Bad Traffic	ET INFO Possible Chrome Plugin install

Debug output strings

No debug info