ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	data.pdf
Full analysis:	https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6
Verdict:	Malicious activity
Analysis date:	July 26, 2024 at 08:20:40
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	generated-doc phishing
Indicators:	
MIME:	application/pdf
File info:	PDF document, version 1.7, 1 pages
MD5:	0D06D5045BC3830E9CB90DE1D46EEF01
SHA1:	C50A73C13C29A392BA00DC8E9DF7B44815E4EEAD
SHA256:	AE5C5FC7FDFED3A2A19405B35FBAE8F3D82D285FC8516963E713171257F2906B
SSDEEP:	3072:TMJMarKKzIW9WSgoMqi/Hq+CGQUf0wyah:IKGNzT9sxqcCGP0gh

Software environment set and analysis options

Launch configuration

Task duration:	120 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	60 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

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

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional 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
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE 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)
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- ProfessionalEdition
- QuickAssist Package
- QuickAssist Package
- RollupFix
- RollupFix
- ServicingStack
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- TabletPCMath Package
- TabletPCMath Package
- UserExperience Desktop Package
- UserExperience Desktop Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package

Behavior activities

MALICIOUS

Phishing has been detected
- msedge.exe (PID: 1560)

SUSPICIOUS

No suspicious indicators.

INFO

An automatically generated document
- Acrobat.exe (PID: 6268)

Checks supported languages
- acrobat_sl.exe (PID: 7320)
- identity_helper.exe (PID: 8952)

Executable content was dropped or overwritten
- AdobeARM.exe (PID: 968)

Application launched itself
- AcroCEF.exe (PID: 5692)
- Acrobat.exe (PID: 6268)
- msedge.exe (PID: 1560)

Reads Microsoft Office registry keys
- Acrobat.exe (PID: 6268)
- msedge.exe (PID: 1560)

Reads Environment values
- identity_helper.exe (PID: 8952)

Reads the computer name
- identity_helper.exe (PID: 8952)

Malware configuration

No Malware configuration.

Static information

TRiD

.pdf | Adobe Portable Document Format (100)

EXIF

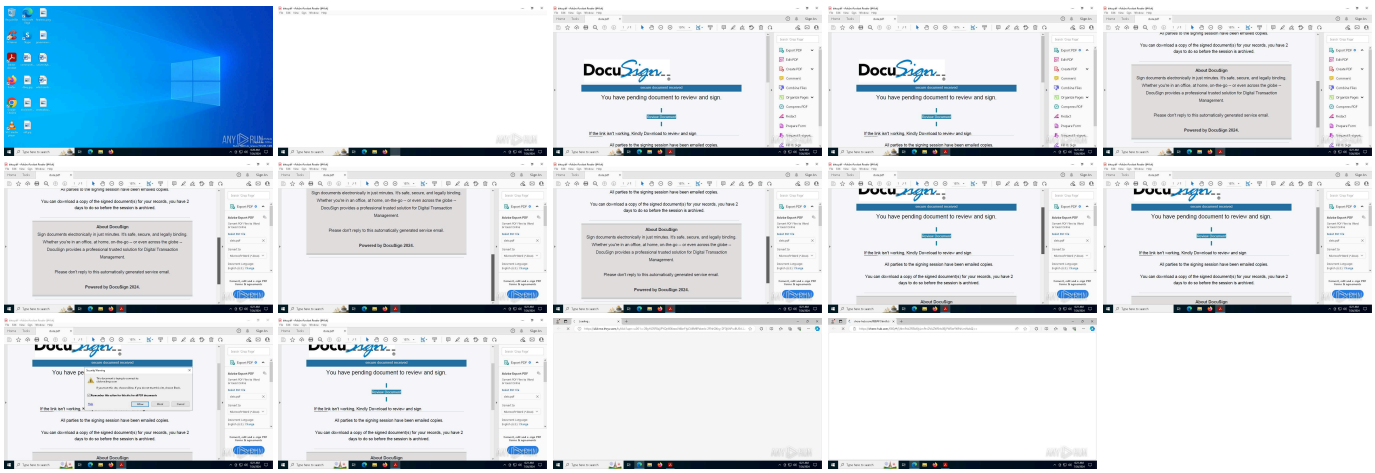
XMP

Producer:	Aspose.Words for Python via .NET 23.11.0
Format:	application/pdf
XMPToolkit:	PDFNet

PDF

Language:	en-US
PageCount:	1
Trapped:	null
ModifyDate:	null0101000000
CreateDate:	null0101000000
Creator:	null
Keywords:	null
Subject:	null
Author:	null
Title:	null
Producer:	-
Linearized:	No
PDFVersion:	1.7

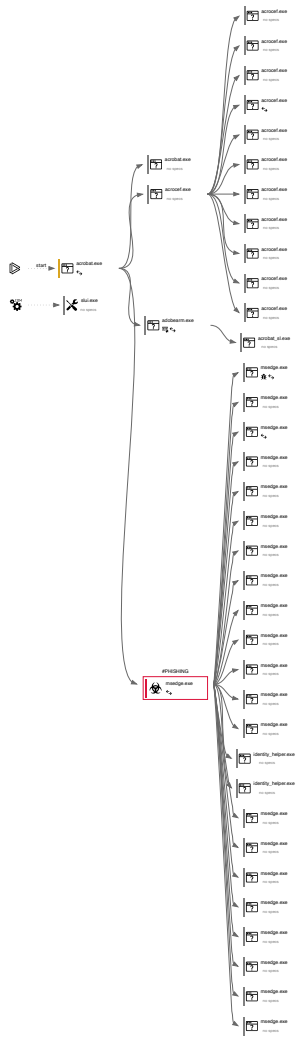
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
183	41	1	1

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
6268	"C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe" C:\Users\admin\AppData\Local\Temp\data.pdf	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe		explorer.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	MEDIUM	**Description:**	Adobe Acrobat
Version:	23.1.20093.0		

6136	"C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe" --type=renderer /prefetch:1 "C:\Users\admin\AppData\Local\Temp\data.pdf"	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe	—	Acrobat.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	LOW	**Description:**	Adobe Acrobat
Version:	23.1.20093.0		

5692	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --backgroundcolor=16514043	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe	—	Acrobat.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	LOW	**Description:**	Adobe AcroCEF
Version:	23.1.20093.0		

6084	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=gpu-process --log-severity=disable --user-agent-product="ReaderServices/23.1.20093 Chrome/105.0.0.0" --lang=en-US --gpu-preferences=UAAAAAAAAADgACAYAAAAAAAAAAAAAAAABgAAAAAAAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEgAAAAAAAAASAAAAAAAAAAYAAAAAgAAABAAAAAAAAAAGAAAAAAAAAAQAAAAAAAAAAAAAAAOAAAAEAAAAAAAAABAAAAADgAAAAgAAAAAAAAAACAAAAAAAAAAA= --log-file="C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\debug.log" --mojo-platform-channel-handle=1568 --field-trial-handle=1596,i,10296150463809524006,13738215573246555272,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:2	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe	—	AcroCEF.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	LOW	**Description:**	Adobe AcroCEF
Exit code:	0	**Version:**	23.1.20093.0

6772	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=gpu-process --log-severity=disable --user-agent-product="ReaderServices/23.1.20093 Chrome/105.0.0.0" --lang=en-US --gpu-preferences=UAAAAAAAAADgACAYAAAAAAAAAAAAAAAABgAAAAAAAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEgAAAAAAAAASAAAAAAAAAAYAAAAAgAAABAAAAAAAAAAGAAAAAAAAAAQAAAAAAAAAAAAAAAOAAAAEAAAAAAAAABAAAAADgAAAAgAAAAAAAAAACAAAAAAAAAAA= --log-file="C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\debug.log" --mojo-platform-channel-handle=1968 --field-trial-handle=1596,i,10296150463809524006,13738215573246555272,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:2	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe	—	AcroCEF.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	LOW	**Description:**	Adobe AcroCEF
Exit code:	0	**Version:**	23.1.20093.0

2124	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=utility --log-severity=disable --user-agent-product="ReaderServices/23.1.20093 Chrome/105.0.0.0" --lang=en-US --log-file="C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\debug.log" --mojo-platform-channel-handle=2120 --field-trial-handle=1596,i,10296150463809524006,13738215573246555272,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:8	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe	—	AcroCEF.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	LOW	**Description:**	Adobe AcroCEF
Version:	23.1.20093.0		

6652	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --log-severity=disable --user-agent-product="ReaderServices/23.1.20093 Chrome/105.0.0.0" --lang=en-US --log-file="C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\debug.log" --mojo-platform-channel-handle=2276 --field-trial-handle=1596,i,10296150463809524006,13738215573246555272,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:8	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe	⇆	AcroCEF.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated

Integrity Level: LOW **Description:** Adobe AcroCEF

Version: 23.1.20093.0

---

704 "C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=renderer --log-severity=disable --user-agent-product="ReaderServices/23.1.20093 Chrome/105.0.0.0" --first-renderer-process --log-file="C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\debug.log" --touch-events=enabled --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=6 --mojo-platform-channel-handle=2088 --field-trial-handle=1596,i,10296150463809524006,13738215573246555272,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:1

C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe — AcroCEF.exe

Information

User: admin **Company:** Adobe Systems Incorporated

Integrity Level: LOW **Description:** Adobe AcroCEF

Version: 23.1.20093.0

3588 "C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=gpu-process --log-severity=disable --user-agent-product="ReaderServices/23.1.20093 Chrome/105.0.0.0" --lang=en-US --gpu-preferences=UAAAAAAAAADgACAYAAAAAAAAAAAAAAAAABgAAAAAAAwAAAAAAAAAAAAAAAA

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	LOW	**Description:**	Adobe AcroCEF
Exit code:	0	**Version:**	23.1.20093.0

4992	C:\WINDOWS\System32\slui.exe -Embedding	C:\Windows\System32\slui.exe	—	svchost.exe

Information

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

2112	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=gpu-process --log-severity=disable --user-agent-product="ReaderServices/23.1.20093 Chrome/105.0.0.0" --lang=en-US --gpu-preferences=UAAAAAAAAADgACAYAAAAAAAAAAAAAAAAABgAAAAAAAwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEgAAAAAAAAASAAAAAAAAAYAAAAAgAAABAAAAAAAAAGAAAAAAAAAAQAAAAAAAAAAAAAAAOAAAAEAAAAAAAAABAAAAADgAAAAgAAAAAAAAACAAAAAAAAAA= --use-gl=disabled --log-file="C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\debug.log" --mojo-platform-channel-handle=2460 --field-trial-handle=1596,i,10296150463809524006,13738215573246555272,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:2	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe	—	AcroCEF.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	LOW	**Description:**	Adobe AcroCEF
Version:	23.1.20093.0		

968	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe" /PRODUCT:Acrobat /VERSION:23.0 /MODE:3	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe		Acrobat.exe

Information

User:	admin	**Company:**	Adobe Inc.
Integrity Level:	MEDIUM	**Description:**	Adobe Reader and Acrobat Manager
Version:	1.824.460.1042		

7320	"C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat_sl.exe"	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrobat_sl.exe	—	AdobeARM.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	MEDIUM	**Description:**	Adobe Acrobat SpeedLauncher
Exit code:	0	**Version:**	22.3.20310.0

7476	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --type=renderer --log-severity=disable --user-agent-product="ReaderServices/23.1.20093 Chrome/105.0.0.0" --log-file="C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\debug.log" --touch-events=enabled --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=12 --mojo-platform-channel-handle=2616 --field-trial-handle=1596,i,10296150463809524006,13738215573246555272,131072 --disable-features=BackForwardCache,CalculateNativeWinOcclusion,WinUseBrowserSpellChecker /prefetch:1	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe	—	AcroCEF.exe

Information

User:	admin	**Company:**	Adobe Systems Incorporated
Integrity Level:	LOW	**Description:**	Adobe AcroCEF
Version:	23.1.20093.0		

1560	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument https://clickme.thryv.com/ls/click?upn=u001.s-2ByHGRFBzjJPYQn83fzoo0t6brFtyCA8V8Pxbmb-2FNrGKny-2F3j6hPsc8U5rLisWgrcFdU_4waRj8OKpDmo7zDlJ9NcHFyU9jrJnIlNfgxRP9s0-2F89LXlXO7ZQgv26r-2FveAJBLIyV1A4h8-2B3DwRaLCJa60yYT6R1uy8VQdo6xsnY5vie-2BuTIAFy1keoO3qYK-2Fxtvu-2Fdc-2FY2R6cgCk0nUXaZi6-2FQ2ClEesMbtPTZlvlpRqLYGwAIN3XGs-2FK-2BfeS790FoFC0RZNnxFzuxzg0PpVB19B-2BbBpUkQBWtkFrJ7I8f2e4l403g9hg1WaJioTg-2FgGw0JrZAWAJVYiWFInzWhQxcu7mQ2oYb06-2BpDoRNaeUbLGxUFllTmw-2B8fkya5x2KvmnAarqRrbATXNAhNxVpjjzdq4AyY31P9LDdUtzf9QHn6wBSDMmsWNrMOf0fciPAzxU7Wq8-2BwZmHI8hhap5LQhxK-2Fm7iow-3D-3D#/?/dm9sb2R5bXlyLm9rc2VuZW5rb0BjYW5wYWNrLmNvbQ==	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		Acrobat.exe

Information

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

Version: 122.0.2365.59

7552 "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=0x300,0x304,0x308,0x2f8,0x310,0x7ffefcf65fd8,0x7ffefcf65fe4,0x7ffefcf65ff0

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		

7928 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --mojo-platform-channel-handle=2428 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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		

7936 "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=3056 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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		

7892 "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=3140 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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		

8056 "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=3548 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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		

7348 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --no-appcompat-clear --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --mojo-platform-channel-handle=3756 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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

5624 "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --extension-process --renderer-sub-type=extension --no-

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

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=4248 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --variations-seed-version /prefetch:2

Information

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

8004 "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=4372 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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

8420 "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=4276 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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:	3221225477	**Version:**	122.0.2365.59

8452 "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=10 --mojo-platform-channel-handle=5036 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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		

8612 "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=4924 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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

8832 "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=5876 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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		

8840 "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=5056 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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		

8936	"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=6388 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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

8952	"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=6388 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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
Version:	122.0.2365.59		

8988	"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=6492 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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

9020	"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=6624 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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

9032	"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=6788 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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

9040	"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=6812 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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

9160	"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=7088 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --variations-seed-version /prefetch:8	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	–	msedge.exe

Information

	User: admin	Company: Microsoft Corporation				
7716	Integrity Level: LOW	Description: Microsoft Edge	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	—	msedge.exe	
	Exit code: 0	Version: 122.0.2365.59				

"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=6156 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --variations-seed-version /prefetch:8

Information

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

7708	"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=4120 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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
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=1540 --field-trial-handle=2452,i,13541024785259085777,13357156151314330614,262144 --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		

Registry activity

Total events	Read events	Write events	Delete events
30 376	30 206	166	4

Modification events

(PID) Process:	(6268) Acrobat.exe	Key:	HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-2034283098-2252572593-1072577386-2659511007-3245387615-27016815-3920691934
Operation:	write	Name:	DisplayName
Value:	Adobe Acrobat Reader Protected Mode		
(PID) Process:	(6136) Acrobat.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\ExitSection
Operation:	write	Name:	bLastExitNormal
Value:	0		
(PID) Process:	(6136) Acrobat.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVEntitlement
Operation:	write	Name:	bSynchronizeOPL
Value:	0		
(PID) Process:	(6136) Acrobat.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVGeneral
Operation:	write	Name:	aDefaultRHPViewMode_L
Value:	Expanded		
(PID) Process:	(6136) Acrobat.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVGeneral
Operation:	write	Name:	bExpandRHPInViewer
Value:	1		
(PID) Process:	(6136) Acrobat.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVGeneral
Operation:	write	Name:	uLastAppLaunchTimeStamp
Value:			
(PID) Process:	(6136) Acrobat.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVGeneral
Operation:	write	Name:	iNumAcrobatLaunches
Value:	3		
(PID) Process:	(6136) Acrobat.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVGeneral
Operation:	write	Name:	iNumUserDockUndockHUD
Value:	0		
(PID) Process:	(6136) Acrobat.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\NoTimeOut

Operation: write **Name:** smailto
Value: 5900

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\ToolsSearch
Operation: write **Name:** iSearchHintIndex
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\DLLInjection
Operation: write **Name:** bBlockDLLInjection
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVEntitlement
Operation: write **Name:** sProductGUID
Value: 4143524F4241545F475549445F4E474C5F44554D4D5900

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVEntitlement
Operation: write **Name:** sProductGUID
Value: 4143524F5F5245534944554500

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AdobeViewer
Operation: delete value **Name:** ProductInfoCache
Value:

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AdobeViewer
Operation: write **Name:** EULAAcceptedForBrowser
Value: 1

(PID) Process: (6268) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AdobeViewer
Operation: delete value **Name:** ProductInfoCache
Value:

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\SessionManagement
Operation: write **Name:** bNormalExit
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\SessionManagement\cWindowsCurrent\cWin0
Operation: write **Name:** iTabCount
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\SessionManagement\cWindowsCurrent
Operation: write **Name:** iWinCount
Value: 1

(PID) Process: (6268) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (6268) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (6268) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (6268) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe ARM\1.0\ARM
Operation: delete value **Name:** iNotify
Value:

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe ARM\1.0\ARM
Operation: write **Name:** iSpeedLauncherLogonTime
Value: 1F184DD6FFD8DA01

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe ARM\1.0\ARM
Operation: write **Name:** iLastProcessedPdfExtension
Value:

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (968) AdobeARM.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe ARM\1.0\ARM
Operation: write **Name:** iLastProcessedMAU
Value:

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cDocumentCenter
Operation: write **Name:** bAlwaysUseServer
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cDocumentCenter
Operation: write **Name:** bAlwaysUseServerFD
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cDocumentCenter
Operation: write **Name:** bDefault
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cDocumentCenter
Operation: write **Name:** bDefaultFD
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cDocumentCenter
Operation: write **Name:** tDistMethod
Value: UPLOAD

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cDocumentCenter\cSettings
Operation: write **Name:** tcSetting
Value: https://api.share.acrobat.com

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cDocumentCenter
Operation: write **Name:** tUI
Value: Adobe online services (Recommended)

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cDocumentCenter
Operation: write **Name:** tURL
Value: urn://ns.adobe.com/Collaboration/SharedReview/Acrobat.com

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cEmailDistribution
Operation: write **Name:** bAlwaysUseServerFD
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cEmailDistribution
Operation: write **Name:** bDefaultFD
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cEmailDistribution
Operation: write **Name:** tDistMethod
Value: EMAIL

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cEmailDistribution\cSettings
Operation: write **Name:** tcSetting
Value:

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cEmailDistribution
Operation: write **Name:** tUI
Value: Manually collect responses in my email inbox

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cEmailDistribution
Operation: write **Name:** tURL
Value: urn://ns.adobe.com/Collaboration/Forms/Email

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInternalServer

Operation: write **Name:** bAlwaysUseServerFD
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInternalServer
Operation: write **Name:** bDefaultFD
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInternalServer
Operation: write **Name:** tDistMethod
Value: InternalServer

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInternalServer\cSettings
Operation: write **Name:** tcSetting
Value:

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInternalServer
Operation: write **Name:** tUI
Value: Automatically collect responses on my own internal server

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInternalServer
Operation: write **Name:** tURL
Value: urn://ns.adobe.com/Collaboration/Forms/InternalServer

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInitiationWizardFirstLaunch
Operation: write **Name:** bIsFirstLaunchER
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInitiationWizardFirstLaunch
Operation: write **Name:** bIsFirstLaunchFD
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInitiationWizardFirstLaunch
Operation: write **Name:** bIsFirstLaunchSF
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInitiationWizardFirstLaunch
Operation: write **Name:** bIsFirstLaunchSR
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Collab\cInitiationWizardFirstLaunch
Operation: write **Name:** bIsFirstLaunchUF
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cHandlers
Operation: write **Name:** aPrivKey
Value: Adobe.PPKLite

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c290FA7E61053E8763C6055E6333A99EFB83ECACB\cAdobe_OCSPRevChecker\cAuthorizedResponder\c0
Operation: write **Name:** bValue
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c0
Operation: write **Name:** iEnd
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c0
Operation: write **Name:** iStart
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c0\cValue
Operation: write **Name:** s0
Value: 312E322E3834302E3131343032312E312E362E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c0\cValue
Operation: write **Name:** s1
Value: 312E322E3834302E3131343032312E312E322E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1
Operation: write **Name:** iEnd
Value: 2

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAccept

ablePolicyOIDs\c1

Operation: write **Name:** iStart

Value: 2

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s0

Value: 312E322E3834302E3131343032312E312E342E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s1

Value: 312E322E3834302E3131343032312E312E342E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s2

Value: 312E322E3834302E3131343032312E312E372E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s3

Value: 312E322E3834302E3131343032312E312E31302E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s4

Value: 312E322E3834302E3131343032312E312E31302E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s5

Value: 312E322E3834302E3131343032312E312E31332E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s6

Value: 312E322E3834302E3131343032312E312E31362E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s7

Value: 312E322E3834302E3131343032312E312E31392E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s8

Value: 312E322E3834302E3131343032312E312E32322E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s9

Value: 312E322E3834302E3131343032312E312E32352E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s10

Value: 312E322E3834302E3131343032312E312E32382E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s11

Value: 312E322E3834302E3131343032312E312E33302E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_OCSPRevChecker\cAuthorizedResponder\c0

Operation: write **Name:** bValue

Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_OCSPRevChecker\cSendNonce\c0

Operation: write **Name:** iValue

Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_OCSPRevChecker\cSignCertOID\c0

Operation: write **Name:** sValue
Value: 312E322E3834302E3131343032312E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_OCSPRevChecker\cSignRequest\c0
Operation: write **Name:** bValue
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E310000\cAdobe_OCSPRevChecker\cURLToConsult\c0
Operation: write **Name:** iValue
Value: 3

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c0
Operation: write **Name:** iEnd
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c0
Operation: write **Name:** iStart
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c0\cValue
Operation: write **Name:** s0
Value: 312E322E3834302E3131343032312E312E362E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c0\cValue
Operation: write **Name:** s1
Value: 312E322E3834302E3131343032312E312E322E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1
Operation: write **Name:** iEnd
Value: 2

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1
Operation: write **Name:** iStart
Value: 2

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s0
Value: 312E322E3834302E3131343032312E312E342E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s1
Value: 312E322E3834302E3131343032312E312E342E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s2
Value: 312E322E3834302E3131343032312E312E372E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s3
Value: 312E322E3834302E3131343032312E312E31302E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s4
Value: 312E322E3834302E3131343032312E312E31302E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s5
Value: 312E322E3834302E3131343032312E312E31332E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue

Operation: write **Name:** s6
Value: 312E322E3834302E3131343032312E312E31362E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s7
Value: 312E322E3834302E3131343032312E312E31392E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s8
Value: 312E322E3834302E3131343032312E312E32322E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s9
Value: 312E322E3834302E3131343032312E312E32352E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s10
Value: 312E322E3834302E3131343032312E312E32382E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_ChainBuilder\cAcceptablePolicyOIDs\c1\cValue
Operation: write **Name:** s11
Value: 312E322E3834302E3131343032312E312E33302E3200

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_OCSPRevChecker\cAuthorizedResponder\c0
Operation: write **Name:** bValue
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_OCSPRevChecker\cSendNonce\c0
Operation: write **Name:** iValue
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_OCSPRevChecker\cSignCertOID\c0
Operation: write **Name:** sValue
Value: 312E322E3834302E3131343032312E3100

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_OCSPRevChecker\cSignRequest\c0
Operation: write **Name:** bValue
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E322E3834302E3131343032312E312E312E310000\cAdobe_OCSPRevChecker\cURLToConsult\c0
Operation: write **Name:** iValue
Value: 3

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E332E33362E382E312E310000\cAdobe_CRLRevChecker\cRequireAKI\c0
Operation: write **Name:** bValue
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E332E33362E382E312E310000\cAdobe_ChainBuilder\cAllowCAToIssueAC\c0
Operation: write **Name:** bValue
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E332E33362E382E312E310000\cAdobe_ChainBuilder\cCheckCABasicConstraints\c0
Operation: write **Name:** bValue
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E332E33362E382E312E310000\cAdobe_OCSPRevChecker\cAllowOCSPNoCheck\c0
Operation: write **Name:** bValue
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E332E33362E382E312E310000\cAdobe_OCSPRevChecker\cRequireOCSPCertHash\c0

Operation: write **Name:** bValue
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cASPKI\cASPKI\cCustomCertPrefs\c312E332E33362E382E312E310000\cAdobe_Validation\cValidityModel\c0
Operation: write **Name:** iValue
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\Security\cPPKHandler
Operation: write **Name:** bCustomPrefsCreated
Value: 1

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\DiskCabs
Operation: write **Name:** bForms_AdhocWorkflowBackup
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\DiskCabs
Operation: write **Name:** bJSCache_GlobData
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\DiskCabs
Operation: write **Name:** bJSCache_GlobSettings
Value: 0

(PID) Process: (6136) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\TrustManager\cDefaultLaunchURLPerms
Operation: write **Name:** tHostPerms
Value: version:2|thryv.com:2

(PID) Process: (6268) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
Operation: write **Name:** CachePrefix
Value:

(PID) Process: (6268) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
Operation: write **Name:** CachePrefix
Value: Cookie:

(PID) Process: (6268) Acrobat.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Operation: write **Name:** CachePrefix
Value: Visited:

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** failed_count
Value: 0

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** state
Value: 2

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\ThirdParty
Operation: write **Name:** StatusCodes
Value:

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\ThirdParty
Operation: write **Name:** StatusCodes
Value: 01000000

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\BLBeacon
Operation: write **Name:** state
Value: 1

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\EdgeUpdate\ClientState\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
Operation: write **Name:** dr
Value: 1

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\StabilityMetrics
Operation: write **Name:** user_experience_metrics.stability.exited_cleanly
Value: 0

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge
Operation: write **Name:** UsageStatsInSample
Value: 1

(PID) Process: (1560) 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: E07944CDB67C2F00

(PID) Process: (1560) msedge.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\ClientStateMedium\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
Operation: write **Name:** usagestats

Value: 0

(PID) Process: (1560) msedge.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\ClientStateMedium\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
Operation: write **Name:** urlstats
Value: 0

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\IEToEdge
Operation: delete value **Name:** DisabledPendingAutoUpdateConsent
Value:

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\Defaults
Operation: write **Name:** is_dse_recommended
Value: 1

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\Defaults
Operation: write **Name:** is_startup_page_recommended
Value: 1

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\EdgeUpdate\ClientState\{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
Operation: write **Name:** lastrun
Value: 13366448475500306

(PID) Process: (1560) 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: B7CB4ECDB67C2F00

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\918686
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {C0601143-3D73-49B6-ACB9-D5157BC7F81B}

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\918686
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {C133BBA9-070C-4DB9-8E97-6A229AF875D0}

(PID) Process: (7552) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Property
Operation: write **Name:** 00180010F429971D
Value: 0100000001000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B2000000000020000000000106600000001000020000000 8FBB77568B008CC9523FDBFD0719FB2866C0E5448612B9652A82FBED0D2846A0000000000E8000000002000020000000862CABB8729A2673790DE1034996D595EA6B0BD5EDEC03E5FFAC723727D610DE8000000046413E2EFEB147888597CCD2B4B2B493C805F1F88E9F93DE89C30F61218203C56A646111E41F3D991B9266AE19286CCBE405247FF73531566CCB5C8A1EDBE319CB72AAA9657BCA0937F198EDB781EE18C527CDEB990D330DB243C2B65A99C3D99471D8D29BFF5599700BB6A484D6C9C32C1B7C478D4198508640CF2D0E4021BA400000009B70C4F37708B1E4C18716AE68E256D577A814892A1126444EA56AC5728C510196AAD06687F4FD6C7B42D9DD0E5C1E5374491E162F4BF97DAD0D7BFAAE5B1AD2

(PID) Process: (7552) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation: write **Name:** DeviceTicket
Value: 0100000001000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B2000000000020000000000106600000001000020000000C364A64D32AFB6FB9867C09E4CFFBB1F49AC824C166C6F8115F05D7C354F6BD3000000000E8000000002000020000000037B4E4E184AB134D4BF0E9585FCA467338D44CFC5DFAE2B13D373F33FD33A7D0200800002C552FE9160509404DD5D1E1DC0083C05B952D711ADFB500135AD03ED6BEA6F2A24B99D6946C9369D30530DA8FE208A599A705BEA2A143F81FC010FC3A0BE7E925559818304651 64EDB65D7FF2BD6210EC48AF98E2D17CF876FD692D1CC92F9A08CA67B37E04250A14A1A97F7CBDD5452E676B1D1076016BBFA59F8595B0145C5EBFE8E7153958782705790B806A853FB7533796E68320534F7C664DE3DACF32A78E85A7C458EFFB8A6A1EAC84B6B8156D2D82EC1658AD1EA2B32707D8D188603286A36B6F57D6B7CA134F2CF11670D26BD3E695638DA47A04F304220AB1C948672EFA35A2CD6DC0ADD6721D456F634975ED14321221A78D7F6D2018A5C488C4D919B8F62360069385708 73EF25759D3C2CAB7EBD5737604B596ECE3C674126495D30793850B585046C19EEADBDA077D4C1AA9E2FFCBF042AA16855AE4FA57C046072358CCE0C2304D368F9F8FCC1F9547933F6E5D6D0FB8BC387B8A9995A2D11CA919A9EC61CA399A3950D5CE7C5F179F3D3EC1CF1558931808503498A74E0384EADE4D7051FF52EB06208F36101B60294EB9BD791899530F5B1B6462E6436F90CE4948AC9B98AFDFF1132015A2790A4551CDBA8975D71816DAEBAA82DFF5DA407D63ADAAECC72ACD3FF8DB0B0AAB6E85B04A5F8694AF91AACFA28A69A2BCCAA815F0CB9CC47F6B27A7C55E8256580638135F6D59148F905C30D7C80D3B1B57AE6299A4668CE1B9F1499D451DDF51D9F1093E50EAC5045710DBBDE99D122CF333C169E45BBEB5080C6187489902847F635AA126DE4B98EFFFF3DF00024428D02B194DE20168205A7C7A638CAFEF3A74105099E217A309F83421B505755C48618AF3E3DFEE0BA8B17B3F0DE1D4539A0B961F381DD7B1B643EEC23A64B308F8185DBD59C365B5A30909316949C9BE99D76853757F77DCB90A5426511C272C7CB0BCFA541961DDD814DEB7BF9FFE1A3B0CD5FAB791777DDB3226C69F3E9C5C301F7DDF5363704B3CD73A87CE9BE6C513435BB59A4E44F2199B0FBA35CAA6CC4FF913FB6E35CB95F8F061C03CB1343F84E12D548709AD5A8617F534C847AA778F3DA9D810E6D5339D961D21438AEB5462A51A5EE3E8474929101A8263D4F898B4CF7EC315E699DD47032BB01F2421D09BDAEEE448FF52E42994974E9140FC1C34CEAAFF1524C25B1407BED4897241B63417E8D5F42F4115ACABF99870ED8F9A739BB800739CF26DD0B2BD281AD130376CC4AFE2BB972D2B383CD3B11A9CF3725F82090C9C7029BC490A19C3FA9D6E326AD6222FCC91FB5521C69002F1DF21F35AEE044594AC2FEF45ACACCE95401FD4CE2070096F3B1BD29D0A64F1BA5FC975D57EBF37D239E1660E35BF5B09AF36C499929FDCBB9990D87D9D49A64E8C221CC57E903251AC861AB8CB0C6E1C3204CA74F209BF4222605E60FF8359579C21C4F46CFF58074EA3BE3FBD3140FBFB0A9B36C7EFE6F3F293D1E77697915CC56D8ADDCD5F685CD0EB46E2862D105345ED6999B5E3BAC04FA519044C2BA60F6E184CC85EFC85AFAB31A74844D4B80440D42907D07EE79550672D420AD18582F905A2609B6C32F9E77DA64059FDAFE753DFE5F22EEA5F59ADE6CEF2B9EC8DC547B99E7098AB07F3CA7F30BD4E182A7C3452692746FB64CE23CE9F98D704FF0BAE927FCFBB7AC650BB7249E4AFC03DBBBF32206FE815B7D6FA0B5FA0C7E1E8D27DC6B0CE313804016D8040B0F7C28CD3BB68B511F8B9FF618697A27982D4D07FC7C3D37F8D3B6E8B91470FE374A9D60B0EA7E4BA0A67706CAA7BA1BA14C7B9517DFE53F7BB7B94CEC60365F4A04B14F4D62FA23CD13D9B69CBFB4FFB78FAEC36337C414AACAFF1FAF055D7882244612F2A7ACECDA4F16329CA36611A59723DF7C1644EA9C623E384676616CEAF8E9DD6EE05CED2C16BE1B849B4E50F4E4A9F57ED550E669E078A8637BADA831BC6D1E113632A58FF98162AA3262DB1DABE82D8F542E1256FD93F30AF963EA8F39BC07D59EC81F8A4CA1AB060C3CD9237D577D2C26E68BA0BAA65E44ECF3942AA2B853F2DA92B0B3DA5D619B10DC3D0FE05810DD7BA9044899F491E87248F24E108DA4A8E3693B0B34015628E70AA24335B6E969B42D3C86752C5DAB1D678604E45BA4FA35DBC575B78BA470E9AFB9A3871216E3F779971BC1CAF382F9AAFB1688056344A6F4C9915A734F9BB3B01C14BF6FE140E1329450680713E87B00A4AF8468D0258438A383F9033522AAA1A32B6FCF7BC2B1D9838C3A923E0B8D68A6C34EF07E152C8FC210DCF3598BCD14F4E15B408DC64981C6ECAD0E3E6BEB16378E0C4324E2ABCC905D8EC05EB2E95D15C59F748FDD9A78D84788B6583E136B5D10CF45F74CC0E357EAECCF910F97EB48D5E8F8711367ED5447C45B533B87A5089EC38A1B9514BB43539AE9F412FB5F6F7785B93361E6EB1ABAE9EEA6CEBACB89F71B74DDADD62573648998843EB1B878E6D30E73F87B70496E9EE4F2CE7B169375F4CA2EA5770EAD15B2EBC5298D1EEA577CBA9A4F7161D9BF765978324705E0A894C9E3D275882191B5EBE29FA10E7417B2C04FB004B5F63833637B4D5FDBE158F68EB34D99457F6053F19D9C9E575A01B477960F9C2DAAC831B4B70483C4BD59324B73166310F28897E3B21C79D5529E6517D047E9DAFC34947041C240B394AC44E00278F35E2FD6CE2368A249202F336110636FE213E7DB756A876453AB35B521BB8BC6D6A15429DC4F10E6868F36763B524A8C7D584C5C0FE129D5FDEB6D3B1923E46A5595EAE652A2290C53F2AFBE35F58185728F1DBAB12E10A788C5FF24D2F3164BE1AD34184E0AA94C09723669E931F694088CBEA3CC6A9B1D3448F7054970582B5475B466CC63C5FF885BD7E5B323E28DDBD8F7F2CF0EB8DC3F729B8EAF8790E9483F437B8DB2ACF074298670E48AE124C71775EF140000000FBE23C1E77ADF96F12C7B23A95477C76296C7F31F4CFAE34EF9EA6F1E06E6764BA6B2E26366D6933173BAEFC3B4305E6E0CA9E4AC4EADA94FC25928FFC15DBE6

(PID) Process: (7552) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation: write **Name:** DeviceId
Value: 00180010F429971D

(PID) Process: (7552) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation: write **Name:** ApplicationFlags
Value: 1

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\918686
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {49E20F82-E000-4251-ABEE-3C64027786A8}

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Feeds
Operation: write **Name:** EdgeMUID

Value: 085638F3A29D64CA3D492CEEA344659C

(PID) Process: (1560) 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: DF508CCEB67C2F00

(PID) Process: (1560) 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: (1560) 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: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\Profiles\Default
Operation: write **Name:** ShortcutName
Value: Profile 1

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\Profiles\Default
Operation: write **Name:** MUID
Value: 085638F3A29D64CA3D492CEEA344659C

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\Profiles\Default
Operation: write **Name:** ProfileErrorState
Value: 0

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Edge\Profiles
Operation: write **Name:** EnhancedLinkOpeningDefault
Value: Default

(PID) Process: (1560) msedge.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowProperties\918686
Operation: write **Name:** WindowTabManagerFileMappingId
Value: {055F4889-66D0-4E0A-850E-F14988ACBCFA}

Files activity

Executable files	Suspicious files	Text files	Unknown types
3	209	49	2

Dropped files

PID	Process	Filename	Type
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SharedDataEvents-journal **MD5:** 2CB79618102F0354A405F6141D7099E3 **SHA256:** 9AC7B5BD96CE6A581F23A25E551A78022C01D999917B7104F1698A1CD1F60DB6	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old~RF1c32df.TMP **MD5:** FCD96552DAA6924F8C1E9C378163E2C9 **SHA256:** E8EC8E1501E489B27B564C363F4E60963DD57180453B35B092A4B3769E7AA5CA	text
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\AdobeFnt23.lst.6136 **MD5:** 366B140BAFC863B7E366AA1E51604759 **SHA256:** CBC8B288DBD2C72432081CF33CEF431572A94C7FB89DBCD59973B99E3871814E	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\LOG.old **MD5:** 002CE9F1C8E638C89460289DFF260E3B **SHA256:** 710FF791CABA4771BFB6DBAFAF141DA47E1F041BC4040CBB7E7F82C69E15AF0C	text
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb\LOG.old~RF1c31c6.TMP **MD5:** E26AF4B6A1AD62E54D67510EEFE20B2C **SHA256:** BF001234CF5F261254DEA1EA459BBFD4A35D15166C765CA3ED9B56D49A04BE1B	text
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Local Storage\leveldb\LOG.old **MD5:** 43D1F53B48631F8B32E040219417874B **SHA256:** AA4C99C362EB18EB8B91EEB8821960807F725E7C5DE1FBABBA7B910BDA3EEEB8	text
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\TESTING **MD5:** DC84B0D741E5BEAE8070013ADDCC8C28 **SHA256:** 81FF65EFC4487853BDB4625559E69AB44F19E0F5EFBD6D5B2AF5E3AB267C8E06	mp3
6268	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\AdobeSysFnt23.lst **MD5:** 366B140BAFC863B7E366AA1E51604759 **SHA256:** CBC8B288DBD2C72432081CF33CEF431572A94C7FB89DBCD59973B99E3871814E	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\SOPHIA.json **MD5:** 79270D9595B259B53E39403366436A8E **SHA256:** AD0552A8B392315C512F6DC945F318AD83B98FB64415C0CED694843A3C5D2083	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SharedDataEvents **MD5:** EF909016B1BA5EAC273665B379C373F6 **SHA256:** 3A55CBE8BF9E787178A505B532E50AC272FD277988898B3113575AAA7C8AE1A8	sqlite
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4a0e94571d979b3c_0 **MD5:** 58E51073F75A31069C742A4070DEAE06 **SHA256:** 398BBC1A4B8EDEA984FC8A803EF6BA5967323A2DA4416145141F6854D46A9027	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bba29d2e6197e2f4_0	binary

		MD5: 3B771D887FA955CE4252B51C9444F2B7 **SHA256:** 09C32A0E05178DC6CC949E58ACCB3A4A45B5AD0BA5EDADF0C86AA93C25858DB2	
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Temp\acrobat_sbx\acroNGLLog.txt **MD5:** A15B236EF29584812433C3F84BCE58E7 **SHA256:** 8E403E8B2ADAE4E215A5FF26A19E2577F362F2E5B9CE6B45F0CE859DE7331EF5	text
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2a426f11fd8ebe18_0 **MD5:** 6BEE96858DE898731A48D7FE0C232309 **SHA256:** B8596C44F0376268C93D90BCBCFD737383DB64B5061D46034470328D34BC368F	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage\LOG.old~RF1c331d.TMP **MD5:** B875B798FCFA464DB41DDC9789BDB161 **SHA256:** F6259A0B5E546CB737118D559D0FBDFFDCEC68AD4F7B95451FED263058606B13	text
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0786087c3c360803_0 **MD5:** 935BF0A65CD193184B84ACF1D2314B75 **SHA256:** DDE8E76F99713DDBCBC4FE5B55DD4B6BDF09908E94AE3FE7BFD163D4BEF35B63	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Session Storage\LOG.old **MD5:** EC382FFF4B7232181CDB8226E9C289C7 **SHA256:** 27BDA724E8E0654E4BDA2F8E98FE399EF826F052F73FBBDB19CDF78954DB9954	text
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\aba6710fde0876af_0 **MD5:** C60D45C5999BB6E052B75F12B8662EA1 **SHA256:** D21C3ACCC5E9E18A261E8BDF0C7284FE7120D227AC6B8F5E4C5429913248CAD8	binary
968	AdobeARM.exe	C:\Windows\Temp\ArmReport.ini **MD5:** C4DBB5797C48D30597D78B6277E06350 **SHA256:** 0AAF07A70C53FB0918539B8CDDE43645CE1E88BC100D899B0718352971F06BCA	text
968	AdobeARM.exe	C:\Users\admin\AppData\Local\Temp\ArmUI.ini **MD5:** B0DF20BAA9DEE27BDBC3285C7D6D4C57 **SHA256:** 76362509A8CA3E4A9FDC854C56674083EF77CA2C53628CE0ACF4BB4C42D73894	text
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\febb41df4ea2b63a_0 **MD5:** 7757E28BC89DB752CD0429366B15CBCC **SHA256:** 3DCBE5260BB5E8C537EC3B1CB297EDE69D856791DA95E37B379486541EA19B6F	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c84d92a9dbce3e0_0 **MD5:** 7FA3B6DFE939B1AF06AF8B997E476D60 **SHA256:** 72B1CB0D3751B8ABF8FC8BF28A3BAADFC54BB42487BFE3E5DF852EBFF2F62F32	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d5dedf551f4d1592_0 **MD5:** 5C0387C8F31F6FE6619D37D0E195C501 **SHA256:** EFDEDA18A21A3702D8CD69FE6B7E7E353E1E76C1AAB0FB31162CEB74A1823B91	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\946896ee27df7947_0 **MD5:** 96148F4832F3BB02DD05DF502AE48D68 **SHA256:** 6161D970F2E19FE0ED10D09221C31961620DA506563574D42A80BF1AE85D367B	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8e417e79df3bf0e9_0 **MD5:** F93DA538E4B14B668F16415946F09A96 **SHA256:** D5331163499A0E373BE0BEF0940701446041AFFF37CB0A9A10DAA9DE5F4AB985	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\d449e58cb15daaf1_0 **MD5:** BB05A6910C19BB22566A5E663EDED35A **SHA256:** DF65DC979A820A770609ED5E8F615F1B1CC4A8520F7FDF0D454949E458CEBA3C	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f941376b2efdd6e6_0 **MD5:** 983800D92E56E6EF912412285C9F02B2 **SHA256:** 5A95C41747027C356C8828711DA9F264BB67674D916C6BEF241E137D1698AAAF	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\8c159cc5880890bc_0 **MD5:** A7CBEE7616C730F9603896D2DA3CDB5B **SHA256:** 125C6216640F281C49F17FC3080C58AA0240F61A4B04D4B38CCE845FABCD9831	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\72d9f526d2e2e7c8_0 **MD5:** 776BFA3C87F44DC6D44CB6FC2CF910BC **SHA256:** E66C4B00E1BFEDC8B79698C6AC5F2F983473A48E6FE2E3D47A411A939FFBB0BF	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\86b8040b7132b608_0 **MD5:** 96E0DA2D7CC432A5A789D7AE0E8DAA6C **SHA256:** 18AFB21C2C900783D2C851D6964692F3D3FA3B65AB5FC37EA26AD37C1F308D4E	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\560e9c8bff5008d8_0 **MD5:** 4172299C761177D8B6E4808B1B601C82 **SHA256:** 55A1C0AE10E7D7DB2EDF6B576ABF2EA1E0AB639CE491CF3A77CED73F67C9093E	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\7120c35b509b0fae_0 **MD5:** 4C989A646C82ADBAE354180E16045D0D **SHA256:** 086FA9D3E9DE3E0D24E00CEB2D3983786D49013039050BF5225152713E6130CE	binary
968	AdobeARM.exe	C:\Users\admin\AppData\Local\Temp\ReportOwner27192.txt **MD5:** 455831477B82574F6BF871193F2F761D **SHA256:** 69BF0BC46F51B33377C4F3D92CAF876714F6BBBE99E754448732792O873F9820	text
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\fd17b2d8331c91e8_0 **MD5:** 43CCB683B21F7C2FCEDB3B7F4539FF21 **SHA256:** 1EB5509D2E6DEB7554FD6424A18FBAAE709CBB530A29AA509E630A50F41348B4	binary
968	AdobeARM.exe	C:\Users\admin\AppData\Local\Temp\ProcessMAU27195.txt **MD5:** 455831477B82574F6BF871193F2F761D **SHA256:** 69BF0BC46F51B33377C4F3D92CAF876714F6BBBE99E754448732792O873F9820	text
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\78bff3512887b83d_0 **MD5:** D97FFB2490AAC53D382CDDB75BCB96A2 **SHA256:** 9D25851CE6BCA149739E7B9233B0D5ED3DFD7ABDAA0BBC4B74557D6DA0BD55AC	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0f25049d69125b1e_0 **MD5:** 7F0F3FAAC8D31DF661D567A1CBD68C8E **SHA256:** 73289471C2521E2D661BA466E70DC01A52B84EAFA716C8338648568A5538AB68	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\92c56fa2a6c4d5ba_0 **MD5:** E05317FD02ECC2B024E68A0F4A57059B **SHA256:** 5138FEA464F61061D9DBA14B1A18159160BA0605C2543A67772A4A907B1B0515	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\983b7a3da8f39a46_0 **MD5:** 57B3D628A96CA05DC190EBCF843959BA **SHA256:** 459476903A0819DE45E2FC1EE1EB40971352A614A63FC2411A70DF6D7033F66C	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0998db3a32ab3f41_0 **MD5:** 1DF898533E524525AABDF4110B16EE07 **SHA256:** 8FF320AC369B94718D879F7DB8D46F54682CEF1FB05B5B67068AB080CF5CBEE2	binary

5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\230e5fe3e6f82b2c_0 **MD5:** 9420950496B8AA0D5EFF6AC9C987B978 **SHA256:** 84276AC9158367644810DA5A8B506CB0C4DD8BA077A177DC0CAE098E7127A937	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_05349744be1ad4ad_0_1 **MD5:** 4B6AF00811DC5EF6A46DA103BDF9BCCD **SHA256:** 4955DB6E947046F22915D128803DB5F7163C9CE19CECC9059100BA394C4A355C	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_56c4cd218555ae2b_0_1 **MD5:** 2EB9BE68AEC9733E5E8B75AA937641CB **SHA256:** DC3A44C3562F707A813D03AFE92E31E182F7850B153701501C0FCDEEADC19D75	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_0998db3a32ab3f41_0_1 **MD5:** 28A3C72CF81C153E32D4616ADDB3DE88 **SHA256:** 6BB2093F79EC6CB1937CB9D16C88519B12D802B2F289F4A72D57BFE1E3494681	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\91cec06bb2836fa5_0 **MD5:** 3BF0BEA622FB010030F4D2F6C67DB346 **SHA256:** 0143D2A34097075FE661BF99A13CE356DEA6275555440D69FC57F4D152750618	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\56c4cd218555ae2b_0 **MD5:** 2EFDE598205A8C0017F2F0AB576A710A **SHA256:** 6C3A4BB6F281BC1D7993CDD90C1CB0BCA2E2EA0632CD48710045493ABE6EB197	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\05349744be1ad4ad_0 **MD5:** C5856CB2F932C4CA8AB6A5622AF6F61C **SHA256:** 0FA19255D2D400532A49B7956C3EF7C5FB9E35F6A65F2A0F060F40189A627C52	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\6fb6d030c4ebbc21_0 **MD5:** B55BE1732B3AE26547C9B102A26C32D1 **SHA256:** B0DB514782C4680E7515F0E2DF9E37DDD1865FD163B7E5411905C8720977E627	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\bf8eae3dcaf681ca_0 **MD5:** E113FD029EE4A8818A111F755738FF79 **SHA256:** 2999E713BA68456F7403DBC8150D104C104DD31C5EAD803268CE271ABAEB8D76	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_927a1596c37ebe5e_0_1 **MD5:** 68942619354E601A61620C7EA817441E **SHA256:** 9CAF175133431E6AE337731B6D81DF2CCECC48E98467148844ADF833B706DBE9	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\todelete_f0cf6dfa8a1afa3d_0_1 **MD5:** 796C33EC074D659A7E595E698304A7DE **SHA256:** F4B19C11E30BCCA82E96C64471115886874FCA1D964B2ED5CC1FCA8746FA49CF	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f971b7eda7fa05c3_0 **MD5:** E695246F87D2E8C7F513CEC7B55740AE **SHA256:** 93223D4A85B32405629475B47B7AE70DEDC138D4F8DD85F54C253C8873CC7A48	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\4ca3cb58378aaa3f_0 **MD5:** C8B599A6C9EDCBEDC4E317EC541A6828 **SHA256:** 58FC678ED0C48B2F9F5E9D76F32E6F47E52129526FF1DC5AC3EC5C0BD1B23893	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\71febec55d5c75cd_0 **MD5:** E7D299A028D394EC1F8B5C090635026C **SHA256:** 13329E33E3672FAD33005520FEBCD408A6862D38941AE8757C1BA16D604D00B6	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\f0cf6dfa8a1afa3d_0 **MD5:** 59F6A5A55B98FA12ABA15B76DD081981 **SHA256:** 1A4EFED1042778B2BD79BCE1E6AAC4D8C0638417178076DD26FADF1FC5DA577C	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\cf3e34002cde7e9c_0 **MD5:** F832B8EE3727B23EC37AE5DAC79C8DF1 **SHA256:** 4C708C1BCD9A3A091CDE21474B2EDAAE15699829EBB8A0B13E931AE2B1FB45AE	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\927a1596c37ebe5e_0 **MD5:** AAAA36250695A76223C12E6ED4C66117 **SHA256:** 1404D988977CD7CBE60F6B2FD8AE27378F440514EEE94A2FF02B5F0EC14A3E43	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\2798067b152b83c7_0 **MD5:** 804FC5768EA1CC99547FCA3E6171FDB2 **SHA256:** ACEEDE6D8A711479EBADB76A89B85D27F0907852887BDA5BBBD6BB3091682DCD	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\0ace9ee3d914a5c0_0 **MD5:** 8953DCDDB75593876D5DEB7AB34B32A1 **SHA256:** 7C55AADDB57ACF303246E167CE83F3D5FBD1351E1F01534832749B4ACC9957A3	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\b6d5deb4812ac6e9_0 **MD5:** EB7C56EBC9590222FBEEDA43FC886FFE **SHA256:** 75C6D53EC0CD591616ABFCB44F46134E990843D0425D718BF84B73D816798198	binary
968	AdobeARM.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B398B80134F72209547439DB21AB308D_A4CF52CCA82D7458083F7280801A3A04 **MD5:** 68245A1B2ED4A40126C676F38A89434E **SHA256:** A533C1706628A491BA388D651E5A78F4865432EFE17470CD71C8CA190A8776E2	der
968	AdobeARM.exe	C:\ProgramData\Adobe\ARM\Acrobat_23.001.20093\AcrobatDCx64Manifest3.msi **MD5:** C019EB64476101D69B69CB7548BF23A7 **SHA256:** FAB62F7F29B7124AC912297EBC0927ABB95FD1E943C08551EABFC9D164F19D39	executable
968	AdobeARM.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8EC9B1D0ABBD7F98B401D425828828CE_54359052731E413C60F1C59EABAD4E05 **MD5:** 9F4CA27EAF7DB750CB4007CF3EC215F6 **SHA256:** 821FBF656B0A1826F9AD2F41160F640E554DABE4AFDEF55C3AEBCAD12C1915A6	binary
968	AdobeARM.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\698460A0B6E60F2F602361424D832905_8BB23D43DE574E82F2BEE0DF0EC47EEB **MD5:** CE9A6874A76DA10D24AD8BC4E20E3CF5 **SHA256:** 5EF7AF52925AD2CFA6954BC78F37C121940DCB88884C12DC5EF330E0FA539929	binary
968	AdobeARM.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C8E534EE129F27D55460CE17FD628216_1130D9B25898B0DB0D4F04DC5B93F141 **MD5:** E6642A6FCF8FD3FBCD2D621728C4F1C5 **SHA256:** 8ED8D126DBBC21D28A82318ACB7D6DF069357BFBE2CA5A2F2B3D155FCFF958CF	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_RHP_Intent_Banner **MD5:** 517C55B6A930E68BAFA5821E77E93971 **SHA256:** 99AC3FD2071DF4CBF871F040298944E40B99E5F4662798AB119EC226C2EDD76F	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\64766d63a539c3ca_0 **MD5:** A5F1A476BE9C611BB94EAC55E635052C **SHA256:** C9258E89718B1486110D720305AC860BE5667A4AD99BCF63DCDFB50DC58AF04C	binary
968	AdobeARM.exe	C:\Users\admin\AppData\Local\Temp\Tmp4138.tmp **MD5:** 0852435D15CCBE2F7B8E3C7DAC5275A1 **SHA256:** F41CB7FECB4A6B6FE8CD629B5D9CBF6C3F36FDB88C094BD45F6B715AD1747B64	binary

968	AdobeARM.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B398B80134F72209547439DB21AB308D_A4CF52CCA82D7458083F7280801A3A04 **MD5:** A1A8C71BD58D6AE00B650AB5365202F5 **SHA256:** 906E4C195345C4085FA97A049975FA35CDBB48C27017BFDEEFD7EDDC6CFCF028	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_RHP_Retention **MD5:** 508EC6C177633BA1F8EC6AA9A4B888BE **SHA256:** D33E9B365F19DBCCAB5FAD0EF888B08AD14AC5EDBC71516BE2B65F87F4A6351B	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_FirstMile_Right_Sec_Surface **MD5:** F577259948ACFD977E15DD2F947DD374 **SHA256:** E95416F931E3DCCAFE6322F1B9034D0CA4EC5356083397E0385C637268448B64	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_READER_LAUNCH_CARD **MD5:** A42449B32F2538A068BF894D6D931E9F **SHA256:** 9882AC0C65AB6C179D97BBE1F9693C9827665CC63400AF6258FB990095A9EF9C	binary
968	AdobeARM.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C8E534EE129F27D55460CE17FD628216_1130D9B25898B0DB0D4F04DC5B93F141 **MD5:** 6E48D7CF3A55820E3C932B8574D7DC9B **SHA256:** 46AD9F16784E9C20235129C8C2D8B19C84E665BE265894A78B2508CF2FF5DFF0	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\ACROBAT_READER_MASTER_SURFACEID **MD5:** 0AAF840A239A1858AF0803526FDB2EF5 **SHA256:** B8C725906494B15CDB323ED555B77F32674AACAA0581308151983EF85849FC00	binary
968	AdobeARM.exe	C:\Users\admin\AppData\Local\Temp\Tmp40D9.tmp **MD5:** 0852435D15CCBE2F7B8E3C7DAC5275A1 **SHA256:** F41CB7FECB4A6B6FE8CD629B5D9CBF6C3F36FDB88C094BD45F6B715AD1747B64	binary
968	AdobeARM.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\AH8CR9J5\AcrobatDCx64Manifest3[1].msi **MD5:** C019EB64476101D69B69CB7548BF23A7 **SHA256:** FAB62F7F29B7124AC912297EBC0927ABB95FD1E943C08551EABFC9D164F19D39	executable
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Disc_LHP_Retention **MD5:** 0FABB500C3F53BAA93AEDFADE75D2B48 **SHA256:** E2C8909781C057DEF13AFDE7B9D2EB9EB612586EF5FD47759B67519FB4BC1D3E	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_More_LHP_Banner **MD5:** 1B11371D7EF9877B0F790E5F39FD804C **SHA256:** B1B683E382CF28623864B7C9DE95EEDD76CA8D0F8C7516585E57E71660A857DE	binary
968	AdobeARM.exe	C:\Users\admin\AppData\Local\Adobe\ARM\Acrobat_23.001.20093\AcrobatDCx64Manifest3.msi **MD5:** C019EB64476101D69B69CB7548BF23A7 **SHA256:** FAB62F7F29B7124AC912297EBC0927ABB95FD1E943C08551EABFC9D164F19D39	executable
968	AdobeARM.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\698460A0B6E60F2F602361424D832905_8BB23D43DE574E82F2BEE0DF0EC47EEB **MD5:** 4C8DCB1F12085EED0C7DD2564288C283 **SHA256:** CA18EF6D5A3187124CF59AA3183CD8E6AF566F38558534A03F980AE1AEB01567	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\e58e492b0f04240a_0 **MD5:** 3341120A4CCCD1F338F8329A8EEA14ED **SHA256:** 35610834DE93B7007624BC96DFBE5177DE097CED0F7B00E4F777488079F48E44	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Upsell_Cards **MD5:** ECFCFBB37D44A115E27D4565295497A9 **SHA256:** BA661D97850E3A0B7DCF455C013E2F2B3DAAB5418B3CB12E6FF4EBCA17DD6C2E	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Edit_LHP_Banner **MD5:** C260B301C2F8579F898A10CD497243A2 **SHA256:** B75A005D61CB74F4E273D72FC14A943D626F3B764BF3AB3552A2F4A21E8F5F3A	binary
968	AdobeARM.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8EC9B1D0ABBD7F98B401D425828828CE_54359052731E413C60F1C59EABAD4E05 **MD5:** A89591448AFC6046B36EE78360F488AE **SHA256:** D667F4399E7463E4236583683C3E7388D10282E117EE1B61C4F9CD49E2ED55A1	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_FirstMile_Home_View_Surface **MD5:** 6F3A936C2373930FF48EF38C1371B928 **SHA256:** 4E86FA78CA0EA14950D316DB22BCBB41FF3C8F43F69B213480F80BDE3E10DEAA	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_RHP_Banner **MD5:** 1A0B65FA2B9087720DC95D48E23A1709 **SHA256:** F70FAFAD6F47FCA745B38C262A2AE2BFBEF28FD2580E75D8F721A20B929AA27F	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\Edit_InApp_Aug2020 **MD5:** 4D9E65541DB71ABF7E6B1BA00986B899 **SHA256:** 5070E5E401C0A8E00F24E0D4D577B35EC3DF9DB2B6336A31B30D80EB8DE6327C	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Sign_LHP_Banner **MD5:** 9122E3D20C3D1B6083B591D4D8DD7A57 **SHA256:** B446E071EB5A7FD4546D34A5BF2CDBE59F28ABFE32F49AB7272901CF66CCC132	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Convert_LHP_Banner **MD5:** 9EACFC3ACFBB2B56900D5FC5E51EE542 **SHA256:** D4657F4A070BBF8FA9F6409085D70E0E9846BDF5410741CEE7A46FAF7C8AFA62	binary
6136	Acrobat.exe	C:\Users\admin\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal **MD5:** A2A977414252495F90EE4C7FBACB5B2F **SHA256:** 9232CF2C35C85C97F074B7789254E8270595C57A6CD6C0C0641F2A9D47B1B86A	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old~RF1c6f7a.TMP **MD5:** — **SHA256:** —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\discounts_db\LOG.old **MD5:** — **SHA256:** —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old~RF1c6f7a.TMP **MD5:** — **SHA256:** —	—
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Temp\acrobat_sbx\A918pezlv_o8cu9c_4qg.tmp **MD5:** 997CE5ED3633E8FF84C2F7D1F0E48E53 **SHA256:** E06C221FB5B43F5A25220D326EB501573C2E0CC9FBB31007BF79054B6F613907	compressed
6652	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Network\TransportSecurity~RF1c6a98.TMP **MD5:** D521E7A39CD6E99F25E02F9F76C13D93 **SHA256:** A8D081072DDD97380E854B9B664EADDCFAFE6C28EE51C435F6D6B99919F1A105	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old~RF1c6f7a.TMP **MD5:** — **SHA256:** —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\parcel_tracking_db\LOG.old	—

		MD5: — SHA256: —	
6136	Acrobat.exe	C:\Users\admin\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages MD5: 435C9B09CB6712D6410CB51C0E1B63BE SHA256: 8AEF23925EA590CC9166CC943911709203891A583FDCE12224FECF11170DAD2B	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF1c6f7a.TMP MD5: 005C277031C1B0811A7C22E5545F4227 SHA256: F5AD9A505D0CF5060329C33E1BDA946F4BE85154AB2D6F06BAE4E586065255C8	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\PersistentOriginTrials\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old~RF1c6f7a.TMP MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\9f9633d5-57c9-45fd-81f3-9a65f6741e3e.tmp MD5: 18D9625A2A4F3A39DDACC70D70A1AEF7 SHA256: B4B4E5BD36164C0C225A79A1B5CF08006DDDC91E0F3A25C6F0494F25BF7B07FF	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old MD5: 8D47F4C77FBB47349AF4F36C74B66DD8 SHA256: 79D068B530FDC14B8156AADBEC722C7F99E9EAB759DB658645FE07F58F494563	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old~RF1c6f8a.TMP MD5: — SHA256: —	—
6136	Acrobat.exe	C:\Users\admin\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Acrobat\Files\DC_Reader_Disc_LHP_Banner MD5: 0AE50664EDFDB3895F82BE817E10A4AE SHA256: 933A899DF608FD321891F984D9E54EF849C67AF3F82F44E31936A346AB2FB2CA	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\settings.dat MD5: 3F5284B4CBCC8535AD94E2112C688055 SHA256: 25FA51603B2AEFF5C6F6629C2FFAD99A0540B57E829B89AFDF5BB43A6801AE3B	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithConnectTokenAndKey\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old~RF1c6ff7.TMP MD5: — SHA256: —	—
6136	Acrobat.exe	C:\Users\admin\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache\915DEAC5D1E15E49646B8A94E04E470958C9BB89.crl MD5: B7A9A5A223B9DCE0E7D10E2B32A0BA07 SHA256: 4EF52E63D45F5230C47DBD3764AA90768F708B24885579375724473BB3FFB255	binary
6136	Acrobat.exe	C:\Users\admin\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache\DF22CF8B8C3B46C10D3D5C407561EABEB57F8181.crl MD5: 152F65AAA856C44E87C8ED561AE43C0F SHA256: 48AC59FC9FA38016B6D5A4CB5D89A2C0CABCD8A0404AF29FBE995B4AA647A292	der
6136	Acrobat.exe	C:\Users\admin\AppData\Roaming\Adobe\Acrobat\DC\Security\addressbook.acrodata MD5: 32FCA302C8B872738373D7CCB1E75FD4 SHA256: CD0DD26304B88C20801FE80B33C49C009E2E5D4411B5D7F83252E1D90CD461C6	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Variations MD5: 16B7586B9EBA5296EA04B791FC3D675E SHA256: 474D668707F1CB929FEF1E3798B71B632E50675BD1A9DCEAAB90C9587F72F680	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\commerce_subscription_db\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old~RF1c6f7a.TMP MD5: 9B26FD6E4A9C387240CD419AF8A25546 SHA256: 56E04B639FE85E4479A6324FFC2B878907B0F93DAD1D2945463FB53059276073	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Version MD5: C7E2197BAE099B13BBB3ADEB1433487D SHA256: 3460EEAF45D581DD43A6E4E17AF8102DDAFF5AEAA88B10099527CF85211629E9	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\20d786b4-6a19-4eb0-b0eb-88ad15878496.tmp MD5: 5058F1AF8388633F609CADB75A75DC9D SHA256: CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old MD5: CFBE0B380683A40B0391872F15486DC3 SHA256: A3E3BA70E6A57387EC3EDBAE9BB13647CCE0FA7E3F619DB307ED207D523DAF33	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\Database\LOG.old MD5: CD2998FACAC0854A879F78E4661FD511 SHA256: 0F13795EAA2A2E5FE3CE1DA78B47B45ECE8E150C9CFA769D53126F156DB22F2C	text
6652	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Network\TransportSecurity MD5: 97915DE8A17A4CBB81A446F7DCA2C2A2 SHA256: A27EC6CD24DA1C1FD5935688DBB79BF4BBEDAB67733D746CBCB55918DD178B8C	binary
6652	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Network\73839c94-a8bc-4693-b184-83f277c92eee.tmp MD5: 97915DE8A17A4CBB81A446F7DCA2C2A2 SHA256: A27EC6CD24DA1C1FD5935688DBB79BF4BBEDAB67733D746CBCB55918DD178B8C	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF1c6ff7.TMP MD5: 18D9625A2A4F3A39DDACC70D70A1AEF7 SHA256: B4B4E5BD36164C0C225A79A1B5CF08006DDDC91E0F3A25C6F0494F25BF7B07FF	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old~RF1c6fb9.TMP MD5: 31EA5376CE170F2D18E8D4D7CC9CF194 SHA256: 6F43AC81B1303CE97F356AD87AFE58E8551B95C62909B42FAC38C641EBE81AD4	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\ed7006ca-f928-4e97-bdbc-7e80e514738b.tmp MD5: 5058F1AF8388633F609CADB75A75DC9D SHA256: CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Site Characteristics Database\LOG.old~RF1c6f8a.TMP MD5: 4C6FC733E77D58FCC3AF918C1CC6E230 SHA256: 1331649B3B5BD65EBE1224AA6B3027E7E706E11FBBF6BB4593207EF2C9ED4156	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old MD5: D5B3B004EF27E69494D5AA0168023A29 SHA256: 9D2FCEFF6EAF79A8449CB27AA62C50C3E97C2E95057A785257F09716FE3E733C	text

1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\metadata\LOG.old~RF1c7101.TMP MD5: CE28C2B08987450A26934AE2AE613968 SHA256: 70465180D13A08E1269FABB3C3278EE089B91A831C29AC13F4DC2D328986F83F	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State MD5: 18D9625A2A4F3A39DDACC70D70A1AEF7 SHA256: B4B4E5BD36164C0C225A79A1B5CF08006DDDC91E0F3A25C6F0494F25BF7B07FF	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Session Storage\LOG.old~RF1c70e2.TMP MD5: 02277F91633E3B6D782BB1BCC4AFDAC3 SHA256: 2F7270944B98C75C9B039F7437A775CC23BFA14A9FB12ABC2257FD4AFA7E49EB	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old~RF1c70a3.TMP MD5: 26E139D5563DAE87F964149F046A2160 SHA256: CEBB6F054FA96D9CCAC3C2FE1C3B573467A5254EB3EF2B755C0521DF315FB65F	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\arbitration_service_config.json MD5: 350ABC86EFB653D78BE8F2FA5D7BDB8C SHA256: C42FB154D987390FCCC0F63DAFCED2BA7242410BADF64D6FF5FDC2FB26D103C9	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\b7b24cfb-d0e2-4fa5-b60a-006c21725043.tmp MD5: 6FB26238A6D5B538DD982F50F4DDD4B4 SHA256: A64A7E9CA278607750B30860428C5A3FB8899E661F3254C3118243A144FB9E70	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old~RF1c7111.TMP MD5: E52EEA2EFF50B0B6FE8ED82DB70AAB53 SHA256: 8953681EC30233F72F3FDDC5E3FA9271A1FDEB997290A63FDAF1381D6557E89C	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old MD5: 8908343BB07BB5E4CF3C75508CA8B247 SHA256: 83E75BB7EAE339620F2791CE20DF882182CE7A4FEA9A46E733866D3594F73EB5	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\shared_proto_db\LOG.old MD5: 99575A346875560525583A346242B427 SHA256: 4A3B1E17C7161E37D7B98144A46465E02B5CC1E0568B4A5BC4B65A2660DF7E9D	text
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports~RF1c72f5.TMP MD5: D751713988987E9331980363E24189CE SHA256: 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	ini
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\default_cloud_config.json MD5: 59C4F296BD9CDF96F7481653449C1512 SHA256: 122ECB5BC96AA21A7D578900EB24E87239FCB05E2E23359401BB04133D5A998E	binary
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\dfe8c040-3fd5-4f94-a655-79f91001dc5d.tmp MD5: D751713988987E9331980363E24189CE SHA256: 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	ini
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\ecc4695a-f00d-414a-9922-daf073d4e0db.tmp MD5: 20D4B8FA017A12A108C87F540836E250 SHA256: 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\load_statistics.db-wal MD5: 182BF2EFC9BA4419CEFE8546DF8BA525 SHA256: 1C4E32635330889517270EC2F4B3152F002F0477B0B15549D9CE5225FB325B7D	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\LOG.old MD5: B65ACC05694C8160C1077206E892622F SHA256: 57A14016EB197980D198FEF2A73B1EC691120C3CA83D50A834661063D071C9B6	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Extension State\LOG.old~RF1c716e.TMP MD5: D984DC548967D1A0BFD37B1675F1181B SHA256: 656C8B02B8C52E55B085A478DC9F33E1C04430C504170A9C9DDE2DC72FD3238B	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync Data\LevelDB\LOG.old MD5: 2272BC21F29587E46ECDD74A24709E43 SHA256: B4EB72784711A412C598068377DF490AAFD8E9D3012E99C3B4036DCDFEC7574E	text
7552	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\reports\1094e330-de3a-4504-84f4-dcd98f12a917.dmp MD5: — SHA256: —	—
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports MD5: D751713988987E9331980363E24189CE SHA256: 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	ini
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\7c69436a-2d75-4abf-ada6-d5be6d61f1cf.tmp MD5: D751713988987E9331980363E24189CE SHA256: 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	ini
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\5a2a7058cf8d1e56c20e6b19a7c48eb2386d141b.tbres MD5: 228E4AE9F8646090D139016A46753E9D SHA256: D16B3C3D249995A1AA7356585E4F7F1D01F229A330ACF8BADEB7E7B29A6385A2	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences~RF1c968a.TMP MD5: 5F974B2BF6F6B3D9FB7CEC8D8ADB29C0 SHA256: 8CE7898561734EA726A7613D5B27698F313C2163C0691ECD6F03B6C381093857	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\aec10588-a5d5-4d2a-81b3-4a7ebd52f75b.tmp MD5: BF04A3733A24A8AF37DCC987891E7D7E SHA256: E7A9850933358EAE5BCAD26796FC6E73F24982B41F763B3BE9A2D8D0FB4BCCF9	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\TokenBroker\Cache\e0495fde257df2ef62ee7e3fdb1ebb9d7ff72300.tbres MD5: 9B77933FA4D2D1B90BF8603809CA6CC2 SHA256: 6CA8B2D0489FA673271D11EC712C1ED865F129A40481CCE557BB59D2A3760FC8	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index MD5: 80D067D7891228D3192028A146812771 SHA256: 7139CC4714EB7F7D308BD2743CA267DB10917B6B56437911F95A44318718B25C	binary
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity~RF1c9978.TMP MD5: 42B21C746E35942BF1553D275B1377C0 SHA256: AF94EFFA0F9410F85A54E2D31E761CF6AD4DDB8E15D56E11848F29306193AC7A	binary
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Cache\Cache_Data\f_00017d MD5: 81A1DC865CDF4DBC683918F7D24BECE5 SHA256: 4B0A45C29D7BEAD7E59DA67C9E42A2DCAEA588F69874D16328DCDECC9C45BFA4	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State~RF1c96b9.TMP MD5: 6FB26238A6D5B538DD982F50F4DDD4B4 SHA256: A64A7E9CA278607750B30860428C5A3FB8899E661F3254C3118243A144FB9E70	binary
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries~RF1c98dc.TMP	binary

		MD5: 20D4B8FA017A12A108C87F540836E250 SHA256: 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\Sdch Dictionaries MD5: 20D4B8FA017A12A108C87F540836E250 SHA256: 6028BD681DBF11A0A58DDE8A0CD884115C04CAA59D080BA51BDE1B086CE0079D	binary
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\177f96c2-4dd5-4941-a711-f2d9bbfd7e8b.tmp MD5: F773DC05C2A29FE77E59A21887E64BAF SHA256: EDC161292F517F1522B055926F227E42E6B6BB1F13C0775E0A5F6C4677E25564	binary
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\TransportSecurity MD5: F773DC05C2A29FE77E59A21887E64BAF SHA256: EDC161292F517F1522B055926F227E42E6B6BB1F13C0775E0A5F6C4677E25564	binary
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\temp-index MD5: 80D067D7891228D3192028A146812771 SHA256: 7139CC4714EB7F7D308BD2743CA267DB10917B6B56437911F95A44318718B25C	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Preferences MD5: E207C18D24E1892C03C562577EB9736A SHA256: A325C36F80D43907EA3D59A89521A2D22CBA197DE723600BC22385D480945EAE	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\05a03ffa-7f7f-4e09-9a10-501c55f5eaf8.tmp MD5: E207C18D24E1892C03C562577EB9736A SHA256: A325C36F80D43907EA3D59A89521A2D22CBA197DE723600BC22385D480945EAE	text
7936	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports~RF1c73a1.TMP MD5: D751713988987E9331980363E24189CE SHA256: 4F53CDA18C2BAA0C0354BB5F9A3ECBE5ED12AB4D8E11BA873C2F11161202B945	ini
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_model_metadata_store\LOG.old~RF1cc58a.TMP MD5: — SHA256: —	—
7552	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\metadata MD5: 734EB78C1CC7A48D517050B5697CED9E SHA256: D3850ECFD9ED6C4CB7B87EC5B9FA25FA94E255479D737133E1895BD1351D96EA	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old MD5: 97D61F5A091146DC7F813CF081DECA6F SHA256: 7E00F31C7AFA1AEDCB859E7C4DB1D995665E5E0AE2777EF1E858A6EBD863D228	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_model_metadata_store\LOG.old MD5: — SHA256: —	—
5692	AcroCEF.exe	C:\Users\admin\AppData\LocalLow\Adobe\AcroCef\DC\Acrobat\Cache\Code Cache\js\index-dir\the-real-index~RF1c9f64.TMP MD5: D6815C77AF62DFA12BA84FDFED4CA521 SHA256: 96197BB85CE7883D2F3608AF12BE7083B6F551DA7E73096C975C437B6FAFC321	binary
7552	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\watson_metadata MD5: 3C5189CD9C1F343D384173C9F2AFBBC9 SHA256: B9BD3692DC33F728B05D8CDA357763497BED26E45528B18977E877C897CB605F	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old~RF1cc5a9.TMP MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\optimization_guide_hint_cache_store\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old~RF1cc5a9.TMP MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AutofillStrikeDatabase\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RF1cc5b9.TMP MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old~RF1cc5d8.TMP MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Asset Store\assets.db\LOG.old~RF1cc2f9.TMP MD5: ABF921FB8E8DEB7385DC90A16864ACAD SHA256: 5CE5E7E93BF8F98B25A84605C802519CBE8ED9A197A3448847C506AC7A3D91B1	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\BudgetDatabase\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RF1cc5e7.TMP MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalDB\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RF1cc5e7.TMP MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old~RF1cc607.TMP MD5: — SHA256: —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old~RF1cc357.TMP MD5: 55D090596845D1D706EDB64B1CB1536A SHA256: 45CD74A88F6B56F7ABDA68B3B7D7E4827B946D7D49EEB517C5714FA51AFFBE8C	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old~RF1cc357.TMP MD5: 279162E139C357A4BBCFBCFDD7A00E88 SHA256: 6B09138C2640F10EE9B088C48A47210A8570C7DCB3CAF340BADE94AC97FE9A0A	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\LOG.old	text

		MD5: D13A40EBCBC658F419A64A2506F4B3E7 **SHA256:** 923B6B5C6CE146B67FDB0AAD13A842DBE6FA9BA5DD93AA8F8952983CA3696BF1	
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\EntityExtractionAssetStore.db\LOG.old **MD5:** BD715F079C51E8C4D9AADFEF70125BD9 **SHA256:** 3DDC987F3DD33EA96D8B1D4E805E3A2D3B84B44C5F8FF0F224791F3ABFE7EDD7	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgePushStorageWithWinRt\LOG.old **MD5:** — **SHA256:** —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old~RF1cc636.TMP **MD5:** — **SHA256:** —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Download Service\EntryDB\LOG.old **MD5:** — **SHA256:** —	—
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AdPlatform\auto_show_data.db\LOG.old~RF1cc3a5.TMP **MD5:** 62A3040C823667CC7C3AB12D4ED11B69 **SHA256:** 984AF0FD1516F836AFB73EC13913F5760B58BF7235F999A7503E5FABB3602CDD	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\AdPlatform\auto_show_data.db\LOG.old **MD5:** 261181051C24DEFFC1C62D8EEC9A3071 **SHA256:** 97FDA91F2345B36351A04190A1E9FD6B0B78A60D1F512A4FD6B1A4F2086B6446	text
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps **MD5:** 4A164D87B3F685E409A55B31861F0AE2 **SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5	tss
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\000010.log **MD5:** 44D47E2EE1C326CAEAA3B4968DE079A3 **SHA256:** 6E011687E16E40CA509B0B60FEBE0D5D0366412609129F980DDC280512375440	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\ba400bbe-0966-4a79-bf3d-c34b8b56bbbd.tmp **MD5:** 4A164D87B3F685E409A55B31861F0AE2 **SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5	tss
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\HubApps~RF1cc3e4.TMP **MD5:** 4A164D87B3F685E409A55B31861F0AE2 **SHA256:** C154099A10D88CB51619FEBD29C92F337D5A4B725E206A6B76F44F2F47CB55F5	tss
1560	msedge.exe	C:\Users\admin\AppData\Local\Temp\cv_debug.log **MD5:** D00480DC5C819A11394F6D8AFFE0C281 **SHA256:** E39F21E666116C873F025CA256488DCBECCBD5EA0E4C679695D73B237C69A80F	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Last Browser **MD5:** A397E5983D4A1619E36143B4D804B870 **SHA256:** 9C70F766D3B84FC2BB298EFA37CC9191F28BEC336329CC11468CFADBC3B137F4	binary
1560	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EdgeCoupons\coupons_data.db\000014.ldb **MD5:** ACA1D986B8F3145FB1DE6313EEE217A4 **SHA256:** C4910321B1F1D648774A87B9F7F5F7014FDB80CAC468481C4B8B4AA7FFE959A0	binary
8840	msedge.exe	C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\EntityExtraction\domains_config.json **MD5:** B46F83E2254BA95907A9C00FE1A865E8 **SHA256:** B48BDC49C169D09882B410E00A0D993BD31A563D3288CA9C71D96E39E84EAC4F	binary

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
15	71	51	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
968	AdobeARM.exe	GET	304	2.19.11.122:80	http://acroipm2.adobe.com/assets/Owner/arm/ReportOwner.txt	unknown	—	—	unknown
968	AdobeARM.exe	GET	304	2.19.11.122:80	http://acroipm2.adobe.com/assets/Owner/arm/ProcessMAU.txt	unknown	—	—	unknown
968	AdobeARM.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSRXerF0eFeSWRripTgTkcJWMm7iQQUaDfg67Y7%2BF8Rhvv%2BYXsliGX0TkICEA0aNA9419AA4In9uq1llt8%3D	unknown	—	—	unknown
968	AdobeARM.exe	GET	404	2.19.11.122:80	http://acroipm2.adobe.com/assets/Owner/arm/2024/7/UC/Other.txt	unknown	—	—	unknown
968	AdobeARM.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBT3xL4LQLXDRDM9P665TW442vrsUQQUReuir%2FSSy4IxLVGLp6chnfNtyA8CEA6bGI750C3n79tQ4ghAGFo%3D	unknown	—	—	unknown
4424	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	—	—	unknown
968	AdobeARM.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfIs%2BLjDtGwQ09XEB1Yeq%2BtX%2BBgQQU7NfjgtJxXWRM3y5nP%2Be6mK4cD08CEAitQLJg0pxMn17Nqb2Trtk%3D	unknown	—	—	unknown
968	AdobeARM.exe	GET	404	2.19.11.122:80	http://acroipm2.adobe.com/assets/Owner/arm/2024/7/OwnerAPI/Rdr.txt	unknown	—	—	unknown
968	AdobeARM.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAbY2QTVWENG9oovp1QifsQ%3D	unknown	—	—	unknown
968	AdobeARM.exe	GET	404	2.19.11.122:80	http://acroipm2.adobe.com/assets/Owner/arm/30/adnme/NoValidReasonForAdnme.txt	unknown	—	—	unknown

5368	SearchApp.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEApDqVCbATUviZV57HIIuIA%3D	unknown	—	—	unknown
3676	backgroundTaskHost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHl3O1J0%3D	unknown	—	—	unknown
5368	SearchApp.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	—	—	unknown
7604	backgroundTaskHost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHl3O1J0%3D	unknown	—	—	unknown
4132	OfficeClickToRun.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDlQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEApDqVCbATUviZV57HIIuIA%3D	unknown	—	—	unknown

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:138	—	—	—	whitelisted
6220	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5368	SearchApp.exe	131.253.33.254:443	a-ring-fallback.msedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
5368	SearchApp.exe	2.22.50.217:443	www.bing.com	Akamai International B.V.	DE	unknown
6412	slui.exe	20.83.72.98:443	—	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
6012	MoUsoCoreWorker.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
1428	RUXIMICS.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6564	slui.exe	20.83.72.98:443	—	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
3952	svchost.exe	239.255.255.250:1900	—	—	—	whitelisted
4	System	192.168.100.255:137	—	—	—	whitelisted
968	AdobeARM.exe	2.19.11.122:80	acroipm2.adobe.com	Elisa Oyj	NL	unknown
6652	AcroCEF.exe	184.28.88.176:443	geo2.adobe.com	AKAMAI-AS	US	unknown
968	AdobeARM.exe	95.101.148.135:443	armmf.adobe.com	Akamai International B.V.	NL	unknown
968	AdobeARM.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
968	AdobeARM.exe	2.19.126.142:443	ardownload3.adobe.com	Akamai International B.V.	DE	unknown
6652	AcroCEF.exe	54.224.241.105:443	p13n.adobe.io	AMAZON-AES	US	unknown
6652	AcroCEF.exe	95.101.148.135:443	armmf.adobe.com	Akamai International B.V.	NL	unknown
6012	MoUsoCoreWorker.exe	51.104.136.2:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	whitelisted
4424	svchost.exe	40.126.32.68:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	unknown
4424	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3296	svchost.exe	40.113.110.67:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5368	SearchApp.exe	13.107.246.45:443	fp-afd-nocache-ccp.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
5368	SearchApp.exe	2.22.50.227:443	www.bing.com	Akamai International B.V.	DE	unknown
5368	SearchApp.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3676	backgroundTaskHost.exe	20.103.156.88:443	fd.api.iris.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	unknown
6268	Acrobat.exe	2.19.11.122:443	acroipm2.adobe.com	Elisa Oyj	NL	unknown
3676	backgroundTaskHost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
5368	SearchApp.exe	92.123.104.61:443	www.bing.com	Akamai International B.V.	DE	unknown
7596	backgroundTaskHost.exe	92.123.104.61:443	www.bing.com	Akamai International B.V.	DE	unknown
5368	SearchApp.exe	204.79.197.222:443	fp.msedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7604	backgroundTaskHost.exe	20.105.99.58:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
7604	backgroundTaskHost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
4132	OfficeClickToRun.exe	52.168.112.67:443	self.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted

4132	OfficeClickToRun.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
1560	msedge.exe	239.255.255.250:1900	—	—	—	whitelisted
7936	msedge.exe	13.107.6.158:443	business.bing.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7936	msedge.exe	13.107.246.45:443	fp-afd-nocache-ccp.azureedge.net	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
7936	msedge.exe	13.107.42.16:443	config.edge.skype.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
7936	msedge.exe	13.107.21.239:443	edge.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
7936	msedge.exe	94.245.104.56:443	api.edgeoffer.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
7936	msedge.exe	13.225.78.66:443	clickme.thryv.com	AMAZON-02	US	unknown
7936	msedge.exe	23.48.23.26:443	bzib.nelreports.net	Akamai International B.V.	DE	unknown
—	—	20.12.23.50:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
—	—	192.250.227.19:443	shore-hub.com	CL-794	US	unknown
7936	msedge.exe	104.21.94.125:443	eb447a5c.bcade5fa149ecc032447e271.workers.dev	—	—	unknown
7616	SIHClient.exe	13.85.23.206:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
7936	msedge.exe	92.123.104.61:443	www.bing.com	Akamai International B.V.	DE	unknown
7936	msedge.exe	192.250.227.19:443	shore-hub.com	—	—	unknown
7616	SIHClient.exe	20.12.23.50:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
7552	msedge.exe	104.208.16.94:443	nw-umwatson.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
1560	msedge.exe	224.0.0.251:5353	—	—	—	unknown

DNS requests

Domain	IP	Reputation
t-ring-fdv2.msedge.net	13.107.237.254	unknown
settings-win.data.microsoft.com	20.73.194.208 51.104.136.2	whitelisted
a-ring-fallback.msedge.net	131.253.33.254	unknown
www.bing.com	2.22.50.217 2.22.50.227 92.123.104.61 92.123.104.64 92.123.104.11 92.123.104.65 92.123.104.59 92.123.104.18 92.123.104.63 92.123.104.7 92.123.104.17 92.123.104.53	whitelisted
google.com	142.250.186.174	whitelisted
acroipm2.adobe.com	2.19.11.122 2.19.11.121	whitelisted
geo2.adobe.com	184.28.88.176	whitelisted
armmf.adobe.com	95.101.148.135	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
ardownload3.adobe.com	2.19.126.142 2.19.126.132	whitelisted
p13n.adobe.io	54.224.241.105 34.237.241.83 18.213.11.84 50.16.47.176	whitelisted
login.live.com	40.126.32.68 40.126.32.74 40.126.32.133 20.190.160.14 40.126.32.140 40.126.32.76 40.126.32.136	whitelisted

client.wns.windows.com	40.126.32.138 40.113.110.67	whitelisted
fp-afd-nocache-ccp.azureedge.net	13.107.246.45	unknown
fd.api.iris.microsoft.com	20.103.156.88	whitelisted
th.bing.com	92.123.104.61 92.123.104.53 92.123.104.64 92.123.104.11 92.123.104.65 92.123.104.63 92.123.104.59 92.123.104.7 92.123.104.17	whitelisted
fp.msedge.net	204.79.197.222	whitelisted
arc.msn.com	20.105.99.58	whitelisted
self.events.data.microsoft.com	52.168.112.67	whitelisted
thryv.com	141.193.213.21 141.193.213.20	whitelisted
edge.microsoft.com	13.107.21.239 204.79.197.239	whitelisted
edge-mobile-static.azureedge.net	13.107.246.45	unknown
config.edge.skype.com	13.107.42.16	whitelisted
clickme.thryv.com	13.225.78.66 13.225.78.37 13.225.78.20 13.225.78.33	shared
business.bing.com	13.107.6.158	whitelisted
api.edgeoffer.microsoft.com	94.245.104.56	whitelisted
bzib.nelreports.net	23.48.23.26 23.48.23.51	whitelisted
slscr.update.microsoft.com	20.12.23.50	whitelisted
shore-hub.com	192.250.227.19	unknown
fe3cr.delivery.mp.microsoft.com	13.85.23.206	whitelisted
eb447a5c.bcade5fa149ecc032447e271.workers.dev	104.21.94.125 172.67.223.175	unknown
nw-umwatson.events.data.microsoft.com	104.208.16.94	whitelisted

Threats

PID	Process	Class	Message
7936	msedge.exe	Not Suspicious Traffic	INFO [ANY.RUN] DNS Query to Cloudflare Worker App
7936	msedge.exe	Misc activity	ET INFO Observed DNS Query to Cloudflare workers.dev Domain
7936	msedge.exe	Misc activity	ET INFO Observed DNS Query to Cloudflare workers.dev Domain

Debug output strings

Process	Message
msedge.exe	[0726/062132.237:WARNING:device_ticket.cc(151)] Timed out waiting for device ticket. Canceling async operation.
msedge.exe	[0726/062133.370:ERROR:filesystem_win.cc(128)] GetFileAttributes C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\attachments\1094e330-de3a-4504-84f4-dcd98f12a917: The system cannot find the file specified. (0x2)
msedge.exe	[0726/062133.379:ERROR:filesystem_win.cc(128)] GetFileAttributes C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\attachments\1094e330-de3a-4504-84f4-dcd98f12a917: The system cannot find the file specified. (0x2)
msedge.exe	[0726/062133.400:ERROR:filesystem_win.cc(128)] GetFileAttributes C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\attachments\1094e330-de3a-4504-84f4-dcd98f12a917: The system cannot find the file specified. (0x2)
msedge.exe	[0726/062133.403:ERROR:filesystem_win.cc(128)] GetFileAttributes C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Crashpad\attachments\1094e330-de3a-4504-84f4-dcd98f12a917: The system cannot find the file specified. (0x2)