Recorded Future® Sandbox

Malware Analysis Report

2025-10-11 08:09

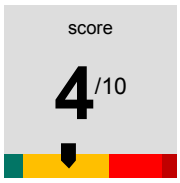
Sample ID	251010-12pgdsvkx5
Target	microsoft word_Rules.xml
SHA256	cb598745eb753980f284741b4ba15dd21f225e4055173df4b83d7b45c4968d1a
Tags	adware discovery spyware

score

4/10

Table of Contents

Part 1. Analysis Overview



SHA256
cb598745eb753980f284741b4ba15dd21f225e4055173df4b83d7b45c4968d1a

Threat Level: Likely benign

The file microsoft word_Rules.xml was found to be: Likely benign.

Malicious Activity Summary

adware	discovery	spyware

Drops file in Windows directory

System Location Discovery: System Language Discovery

Browser Information Discovery

Modifies Internet Explorer settings

Enumerates system info in registry

Suspicious behavior: AddClipboardFormatListener

Modifies registry class

Suspicious behavior: EnumeratesProcesses

Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary

Modifies data under HKEY_USERS

Suspicious use of FindShellTrayWindow

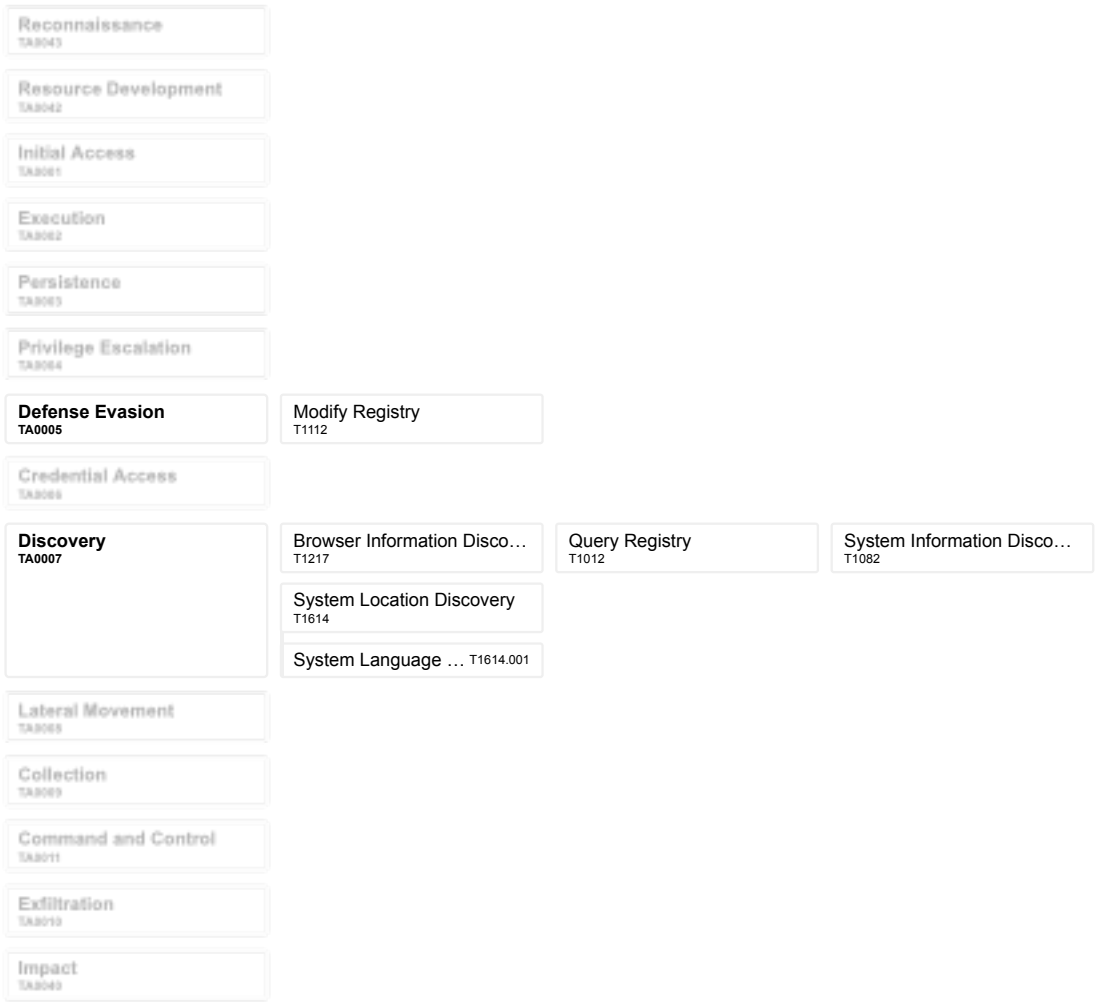
Suspicious use of SetWindowsHookEx

Suspicious use of WriteProcessMemory

Checks processor information in registry

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16



Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-10-10 22:08

3. 2. Signatures

N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-10 22:08	2025-10-10 22:11	win10v2004-20250502-en	149s	148s

4. 2. Command Line

```
"C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE" /verb open "C:\Users\Admin\AppData\Local\Temp\microsoft word_Rules.xml"
```

4. 3. Signatures

System Location Discovery: System Language Discovery

discovery

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A

Modifies Internet Explorer settings

adware spyware

Description	Indicator	Process	Target
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\DomainSuggestion\NextUpdateDate = "466899141"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\Main	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\Recovery\AdminActive\{C947A2F0-A625-11F0-AF61-4A624F806949} = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\Main\FullScreen = "no"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\IESettingSync	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime = "31210034"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\VersionManager	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\TabbedBrowsing	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\Main\WindowsSearch\Version = "WS not running"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime = "2647068542"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\DomainSuggestion	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\Recovery\AdminActive	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\Main\WindowsSearch	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\VersionManager	C:\Program Files\Internet Explorer\iexplore.exe	N/A

Description	Indicator	Process	Target
Set value (data)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue = 01000000d08c9ddf0115d1118c7a00c04fc297eb01000000cd934f5604bc7341a2b6214c393c8229000000000200000000001066000000010000200000007e70a45b491b9bd11a1fcf77c683f6bd1bfb0af6049af43130e1c09f98d02c1e000000000e8000000002000020000000a15b7555144b76a81bed99effe8850c04a650c95debcf5664f07eba636414bfa20000000d19788caf59c818447ed4cf8da46fef87f14db9303f788f1b24eb2e6bccf08f040000000e234a090daa2ccd768868afc8c6723da8d15264484cc1580732723624f2f230e1c3f07d3b270ae8c95e883553bbb8681c8ef3d95be947d0fdf6cc670e6cc4927	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\Main\WindowsSearch	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\DomainSuggestion\FileNames\	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\DomainSuggestion\FileNames\en-US = "en-US.1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\Recovery\PendingRecovery\AdminActive = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NTPFirstRun = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\DecayDateQueue = 01000000d08c9ddf0115d1118c7a00c04fc297eb01000000cd934f5604bc7341a2b6214c393c8229000000000200000000001066000000010000200000029f3c4e4c23e187daf6d44ca10b6b1a881756d5b360a69244265a4fb397e0661000000000e8000000002000020000000004b5b87390000d22f3b32b69dd364af07143468b04738efb81fe33a6f0e41711b200000001ba8a9e846de15727f13969c4e10f0e0fdd54a93b2094bb1535a368098dbe105400000002c5234a217bf194c186d4dca597f10c759c4ace1e17088d5d76a7efaad63417428aa88090aac8df7a6c1c58d4e3a6376fac24fa9772ed369c143347a2b214895	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\DomainSuggestion	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\Recovery\PendingRecovery	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\GPU	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\Main\WindowsSearch\Version = "WS not running"	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\IESettingSync\SlowSettingTypesChanged = "2"	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed = c04e8f9e323adc01	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\DomainSuggestion\FileNames	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\DomainSuggestion\FileNames\	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\Main\CompatibilityFlags = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\Software\Microsoft\Internet Explorer\Main	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\Main\Window_Placement = 2c000000020000000300000fffffffffffffffffffffffffffffffff2400000024000000aa04000089020000	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\GPU\AdapterInfo = "vendorId=\"0x10de\",deviceID=\"0x8c\",subSysID=\"0x0\",revision=\"0x0\",version=\"10.0.19041.546\"hypervisor=\"No Hypervisor (No SLAT)\""	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateLowDateTime = "2653318701"	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\VersionManager\LastCheckForUpdateHighDateTime = "31210034"	C:\Program Files (x86)\Internet Explorer\IEXPL	N/A

Description	Indicator	Process	Target
		ORE.EXE	
Set value (data)	\REGISTRY\USER\S-1-5-21-1153236273-2212388449-1493869963-1000\SOFTWARE\Microsoft\Internet Explorer\TabbedBrowsing\NewTabPage\LastProcessed = b009949e323adc01	C:\Program Files\Internet Explorer\iexplore.exe	N/A

Suspicious use of FindShellTrayWindow

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Internet Explorer\iexplore.exe	N/A

Suspicious use of SetWindowsHookEx

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Internet Explorer\iexplore.exe	N/A
N/A	N/A	C:\Program Files\Internet Explorer\iexplore.exe	N/A
N/A	N/A	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
N/A	N/A	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
N/A	N/A	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A
N/A	N/A	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 3100 wrote to memory of 3056	N/A	C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE	C:\Program Files\Internet Explorer\iexplore.exe
PID 3100 wrote to memory of 3056	N/A	C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE	C:\Program Files\Internet Explorer\iexplore.exe
PID 3056 wrote to memory of 3252	N/A	C:\Program Files\Internet Explorer\iexplore.exe	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
PID 3056 wrote to memory of 3252	N/A	C:\Program Files\Internet Explorer\iexplore.exe	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
PID 3056 wrote to memory of 3252	N/A	C:\Program Files\Internet Explorer\iexplore.exe	C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE

4. 4. Processes

C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE

```
"C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE" /verb open "C:
\Users\Admin\AppData\Local\Temp\microsoft word_Rules.xml"
```

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

```
"C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\Admin\AppData\Local\Temp\microsoft word_Rules.xml
```

C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE

```
"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:3056 CREDAT:17410 /prefetch:2
```

4. 5. Network

Country	Destination	Domain	Proto
US	150.171.28.10:443	ieonline.microsoft.com	tcp
US	8.8.8.8:53	c.pki.goog	udp
GB	142.251.29.94:80	c.pki.goog	tcp

4. 6. Files

memory/3100-0-0x00007FFB59970000-0x00007FFB59980000-memory.dmp

memory/3100-3-0x00007FFB9998D000-0x00007FFB9998E000-memory.dmp

memory/3100-2-0x00007FFB59970000-0x00007FFB59980000-memory.dmp

memory/3100-5-0x00007FFB59970000-0x00007FFB59980000-memory.dmp

memory/3100-4-0x00007FFB59970000-0x00007FFB59980000-memory.dmp

memory/3100-1-0x00007FFB59970000-0x00007FFB59980000-memory.dmp

memory/3100-8-0x00007FFB998F0000-0x00007FFB99AE5000-memory.dmp

memory/3100-7-0x00007FFB998F0000-0x00007FFB99AE5000-memory.dmp

memory/3100-9-0x00007FFB998F0000-0x00007FFB99AE5000-memory.dmp

memory/3100-6-0x00007FFB998F0000-0x00007FFB99AE5000-memory.dmp

memory/3100-10-0x00007FFB998F0000-0x00007FFB99AE5000-memory.dmp

memory/3100-12-0x00007FFB59970000-0x00007FFB59980000-memory.dmp

memory/3100-11-0x00007FFB59970000-0x00007FFB59980000-memory.dmp

memory/3100-13-0x00007FFB998F0000-0x00007FFB99AE5000-memory.dmp

C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B398B80134F72209547439DB21AB308D_9F6005AF34C7906F717D420F892FD6D0

MD5	0a022a2584d63387bdf33e58b8f12479
SHA1	d54be7d9a9f94646c42e19bcd311324c843790cd
SHA256	8fe8839c99ec77e8cf204db640c19685a598e1a614cd8e6108341901b858a06d
SHA512	d53040ba17f07dc510375fcfc9b3e431ebfe9c915b9eabaa43294fc52d91b222536201d90627767ff96464a10df20cceb1b9907bce5397f90b9cb3c634383bb1

C:\Users\Admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B398B80134F72209547439DB21AB308D_9F6005AF34C7906F717D420F892FD6D0

MD5	3bccfaee91dac3ab47cc3e2bff50a822
SHA1	d8d61c0967b948a6a1de17c389d048b494af51b4
SHA256	383a3e68f068b0c4ad641f9da17e356a50f05ffce9cc1fafa60e2a5a4d1c77b9
SHA512	512ac50f1a68738dfc666c5c54b9c4ae76df5262c474a38b9b36c570e4b48a788b29b06dba4ee4c766164064d2cf44eccc1fea0ee91ede4fd8668065e854bd82

C:\Users\Admin\AppData\Local\Microsoft\Windows\INetCache\IE\XVPSC8PT\suggestions[1].en-US

MD5	5a34cb996293fde2cb7a4ac89587393a
SHA1	3c96c993500690d1a77873cd62bc639b3a10653f
SHA256	c6a5377cbc07eece33790cfc70572e12c7a48ad8296be25c0cc805a1f384dbad
SHA512	e1b7d0107733f81937415104e70f68b1be6fd0ca65dccf4ff72637943d44278d3a77f704aedff59d2dbc0d56a609b2590c8ec0dd6bc48ab30f1dad0c07a0a3ee

Part 5. Analysis: behavioral2

5. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-10 22:08	2025-10-10 22:12	win11-20250610-en	149s	142s

5. 2. Command Line

```
"C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE" /verb open "C:\Users\Admin\AppData\Local\Temp\microsoft word_Rules.xml"
```

5. 3. Signatures

Drops file in Windows directory

Description	Indicator	Process	Target
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\th\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\af\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\de\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\sl\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\vi\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1992216217\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1919145674\manifest.fingerprint	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\fa\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\es_419\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\cs\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\zu\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862\dasherSettingSchema.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862\offscreendocument.html	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\hy\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\sk\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\pa\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862\page_embed_script.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1145337351\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1919145674\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\bg\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\hu\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\pt_PT\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\fil\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\hi\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\ko\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\gu\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File opened for modification	C:\Windows\SystemTemp	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Description	Indicator	Process	Target
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862\128.png	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\kk\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\km\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\sw\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\ur\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\el\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862\service_worker_bin_prod.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\eu\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\ro\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_metadata\verified_contents.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1145337351\LICENSE	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1145337351\manifest.fingerprint	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1919145674\LICENSE	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1919145674_metadata\verified_contents.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_409228308\deny_domains.list	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\cy\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\si\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\my\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\ta\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\da\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862\offscreendocument_main.js	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1145337351\sets.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_409228308\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\pt_BR\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\bn\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\ar\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\az\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862\manifest.fingerprint	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_409228308\manifest.fingerprint	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\ka\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\fr\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\et\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\id\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\iw\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\nl\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862_locales\tr\messages.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
File created	C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1294128862\manifest.json	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Browser Information Discovery

discovery

Checks processor information in registry

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

Enumerates system info in registry

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

Modifies Internet Explorer settings

adware spyware

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\CVListXMLVersionLow = "395196024"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\CVListXMLVersionHigh = "268435456"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\GPU\Revision = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersionHigh = "268435456"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\StaleCompatCache = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Main\CompatibilityFlags = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Main	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\TabbedBrowsing\NTPMigrationVer = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersionLow = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\GPU\VendorId = "4318"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersionLow = "395196024"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\VersionManager	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Main\DisableFirstRunCustomize = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Main	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\GPU\DeviceId = "140"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\GPU\SubSysId = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Protected - It is a violation of Windows Policy to modify. See aka.ms/browserpolicy	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\StaleCompatCache = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\GPU	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\VersionManager\FirstCheckForUpdateHighDateTime = "31210039"	C:\Program Files\Internet Explorer\iexplore.exe	N/A

Description	Indicator	Process	Target
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Protected - It is a violation of Windows Policy to modify. See aka.ms/browserpolicy\HomepagesUpgradeVersion = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Main\DisableFirstRunCustomize = "1"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Main\OperationalData = "8"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\CVListDomainAttributeSet = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\TabbedBrowsing	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Main\OperationalData = "9"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\BrowserEmulation\IECompatVersionHigh = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\GPU\SoftwareFallback = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Main\OperationalData = "13"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\Main\CompatibilityFlags = "0"	C:\Program Files\Internet Explorer\iexplore.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000\Software\Microsoft\Internet Explorer\VersionManager\FirstCheckForUpdateLowDateTime = "1639389804"	C:\Program Files\Internet Explorer\iexplore.exe	N/A

Modifies data under HKEY_USERS

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry\TraceTimeLast = "134046077772439750"	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Modifies registry class

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\Shell	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\IconSize = "16"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots = 02020202020202	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\FFlags = "18874369"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\Shell\SniffedFolderType = "Documents"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\ColInfo = 00000000000000000000000000000000 0fddfdffd10000000000000000000000040000001800000030f125b7ef471a10a5f102608c9eebac0a000000100100003 0f125b7ef471a10a5f102608c9eebac0e00000090000000030f125b7ef471a10a5f102608c9eebac0400000078000000 30f125b7ef471a10a5f102608c9eebac0c00000050000000	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A

Description	Indicator	Process	Target
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2 = e7021f006d02d5dfa3235f020400000000005b0200003153505305d5cdd59c2e1b10939708002b2cf9ae97010000120000000041007500740006f004c006900730074000000420000001e000000700072006f00700003400320039003400390036003700320039003500000000000050010000aea54e38e1ad8a4e8a9b7bea78fff1e906000080000000000100000002000080010000000100000002000000200000000000000500014001f50e04fd020ea3a6910a2d808002b30309d3a002e80922b16d365937a46956b92703aca08af260001002600efbe1100000048de60419cdadb019492c101a9dadb014784c7d6323adc01140000000000000000000000000000000000000000000000010000000100008001000000040069007400650006d000000000000000000000000000000000000000000000000000000000000000000000000000042180136ccdcfe40aa3d6177ea401788ffffffffffffffffffffffff000000000010000001b005300650061007200630068002000520065007300750006c0074007300200069006e00200044006f00630075006d0065006e00740073000000000000000000000000000000000000000000000000000000000000390000002400000000410075007400006f006c00690073007400430061006300680065005400690006d00650000000140000009566d2a00d0000006f000000220000000041007500740006f006c006900730074004300610063006800065004b006500790000001f0000001d000000530065006100720063006800200052006500730075006c00740073002000690006e00200044006f00630075006d0065006e007400730030000000000000000000000000000000741a595e96dfd3488d671733bcee28ba671b730433d90a4590e64acd2e9408fe2a0000001300efbe00000020000000000000000000000000000000000000000000000000010000093022a0000001900efbe42180136ccdcfe40aa3d6177ea401788ab814c427b7ac14fa848ddbadc10cdf593020000	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\Mode = "8"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Key created	\REGISTRY\MACHINE\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-2238466657-712128251-1221219315-1000\{CA6A6A5B-38A0-43A0-B4C2-3B643B9505E2}	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\NodeSlot = "6"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\Sort = 000000000000000000000000000000003000000901c6949177e1a10a91c08002b2ecda903000000ffffffff30f125b7ef471a10a5f102608c9eebac0e000000ffffffff30f125b7ef471a10a5f102608c9eebac0a00000001000000	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\GroupByDirection = "1"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\FFlags = "1"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Key created	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance\	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\Mode = "4"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\GroupByKey:FMTID = "{00000000-0000-0000-0000-000000000000}"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A

Description	Indicator	Process	Target
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\GroupByDirection = "1"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\ColInfo = 00000000000000000000000000000000 0fddfdffd1000000000000000000000000500000018000000030f125b7ef471a10a5f102608c9eebac0a000000a000000030f125b7ef471a10a5f102608c9eebac0e0000009000000030f125b7ef471a10a5f102608c9eebac040000007800000030f125b7ef471a10a5f102608c9eebac0c000000500000004c58e0e388b75a4abb207f5a44c9acdd0600000078000000	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\GroupView = "0"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (str)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\GroupByKey:FMTID = "{00000000-0000-0000-0000-000000000000}"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\LogicalViewMode = "1"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\Sort = 00000000000000000000000000000001 00000030f125b7ef471a10a5f102608c9eebac0a00000001000000	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\GroupByKey:PID = "0"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\NodeSlot = "7"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\IconSize = "32"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\GroupByKey:PID = "0"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots = 0202020202	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1 = 3a002e80922b16d365937a46956b92703aca08af260001002600efbe1100000048de60419cdadb019492c101a9dadb014784c7d6323adc0114000000	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\MRUListEx = 01000000000000000ffffffff	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx = 01000000000000000ffffffff	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\FFlags = "1092616193"	C:\Program Files\Microsoft Office\root\Of	N/A

Description	Indicator	Process	Target
		fice16\EXCEL.EXE	
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\MuiCache	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\MiniSearchHost.exe	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\NodeSlots = 020202020202	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\MRUListEx = ffffffff	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6\ComDlg\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\GroupView = "0"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx = 020000000100000000000000ffffffff	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (data)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx = ffffffff	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Set value (int)	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\7\ComDlg\{36011842-DCCC-40FE-AA3D-6177EA401788}\LogicalViewMode = "5"	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
Key created	\REGISTRY\USER\S-1-5-21-2238466657-712128251-1221219315-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\6	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A

Suspicious behavior: AddClipboardFormatListener

Description	Indicator	Process	Target
N/A	N/A	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A

Suspicious behavior: EnumeratesProcesses

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

Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary

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

Suspicious use of FindShellTrayWindow

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

Suspicious use of SetWindowsHookEx

Description	Indicator	Process	Target

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\MiniSearchHost.exe	N/A
N/A	N/A	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A
N/A	N/A	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 3812 wrote to memory of 3916	N/A	C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE	C:\Program Files\Internet Explorer\iexplore.exe
PID 3812 wrote to memory of 3916	N/A	C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE	C:\Program Files\Internet Explorer\iexplore.exe
PID 3916 wrote to memory of 3040	N/A	C:\Program Files\Internet Explorer\iexplore.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3916 wrote to memory of 3040	N/A	C:\Program Files\Internet Explorer\iexplore.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 2268	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 2268	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 4828	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 4828	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Description	Indicator	Process	Target
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 1488	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 4956	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 4956	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 4956	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 4956	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 3040 wrote to memory of 4956	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

5. 4. Processes

C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE

```
"C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE" /verb open "C:
\Users\Admin\AppData\Local\Temp\microsoft word_Rules.xml"
```

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

```
"C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\Admin\AppData\Local\Temp\microsoft word_Rules.xml
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" -- "file:///C:/Users/Admin/AppData/Local/Temp/microsoft%20word_Rules.xml"
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:
\Users\Admin\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:
\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-
version=133.0.6943.99 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 --annotation=prod=Edge
--annotation=ver=133.0.3065.69 --initial-client-data=0x2e4,0x2e8,0x2ec,0x2e0,0x2f4,0x7ffcf192f208,0x7ffcf192f214,0x7ffcf192f220
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --
service-sandbox-type=none --string-annotations --always-read-main-dll --field-trial-handle=1804,i,707768139419494070 2,18240694538911135317,262144 --
variations-seed-version --mojo-platform-channel-handle=2092 /prefetch:11
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --string-annotations --gpu-
preferences=UAAAAAAAAADgAAAEAAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAAAAA --
always-read-main-dll --field-trial-handle=2064,i,707768139419494070 2,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-
handle=2060 /prefetch:2
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --
service-sandbox-type=service --string-annotations --always-read-main-dll --field-trial-handle=1836,i,707768139419494070 2,18240694538911135317,262144
--variations-seed-version --mojo-platform-channel-handle=2472 /prefetch:13
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --pdf-upsell-enabled --video-capture-use-gpu-
memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --
renderer-client-id=6 --always-read-main-dll --field-trial-handle=3428,i,707768139419494070 2,18240694538911135317,262144 --variations-seed-version --
mojo-platform-channel-handle=3464 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --pdf-upsell-enabled --video-capture-use-gpu-
memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --
renderer-client-id=5 --always-read-main-dll --field-trial-handle=3444,i,707768139419494070 2,18240694538911135317,262144 --variations-seed-version --
mojo-platform-channel-handle=3460 /prefetch:1
```

C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.69\elevation_service.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.69\elevation_service.exe"
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.mojom.AssetStoreService --lang=en-US --
service-sandbox-type=asset_store_service --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=4696,i,707768139419494070 2,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=4888 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity_extraction_service.mojom.Extractor --
lang=en-US --service-sandbox-type=entity_extraction --onnx-enabled-for-ee --video-capture-use-gpu-memory-buffer --string-annotations --always-read-
main-dll --field-trial-handle=4744,i,707768139419494070 2,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=4912 /
prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US
--service-sandbox-type=service --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=5628,i,707768139419494070 2,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=5632 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.ProfileImport --lang=en-US --service-
sandbox-type=none --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=5788,i,707768139419494070 2,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=5800 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.69\identity_helper.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.69\identity_helper.exe" --type=utility --utility-sub-
type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --video-capture-use-gpu-memory-buffer --string-annotations --
always-read-main-dll --field-trial-handle=5840,i,707768139419494070 2,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-
handle=5868 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.69\identity_helper.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.69\identity_helper.exe" --type=utility --utility-sub-
type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --video-capture-use-gpu-memory-buffer --string-annotations --
always-read-main-dll --field-trial-handle=5840,i,707768139419494070 2,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-
handle=5868 /prefetch:14
```

C:\Program Files (x86)\Microsoft\Edge\Application\133.0.3065.69\cookie_exporter.exe

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

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-
sandbox-type=service --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=5676,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=6148 /prefetch:14
```

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

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

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.mojom.DataDecoderService --lang=en-US
--service-sandbox-type=service --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=6324,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=6292 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-
sandbox-type=none --message-loop-type-ui --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=5880,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=5904 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-
sandbox-type=none --message-loop-type-ui --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=5928,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=6236 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=chrome.mojom.UtilWin --lang=en-US --service-
sandbox-type=none --message-loop-type-ui --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=5872,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=6216 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-
type=edge_search_indexer.mojom.SearchIndexerInterfaceBroker --lang=en-US --service-sandbox-type=search_indexer --message-loop-type-ui --video-
capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=4964,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=2884 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-
sandbox-type=service --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=5548,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=5724 /prefetch:14
```

C:\Windows\System32\rundll32.exe

```
C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-
sandbox-type=service --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-
handle=1996,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=6132 /prefetch:14
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=entity_extraction_service.mojom.Extractor --
lang=en-US --service-sandbox-type=entity_extraction --onnx-enabled-for-ee --video-capture-use-gpu-memory-buffer --string-annotations --always-read-
main-dll --field-trial-handle=884,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=4908 /
prefetch:14
```

C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE

```
"C:\Program Files\Microsoft Office\Root\VFS\ProgramFilesCommonX64\Microsoft Shared\Office16\MSOXMLED.EXE" /verb open "C:
\Users\Admin\AppData\Local\Temp\microsoft word_Rules.xml"
```

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

```
"C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\Admin\AppData\Local\Temp\microsoft word_Rules.xml
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" -- "file:///C:/Users/Admin/AppData/Local/Temp/microsoft%20word_Rules.xml"
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --string-annotations --pdf-upsell-enabled --video-capture-use-gpu-
memory-buffer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --
renderer-client-id=21 --always-read-main-dll --field-trial-handle=6472,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version
--mojo-platform-channel-handle=4928 /prefetch:1
```

C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\MiniSearchHost.exe

```
"C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\MiniSearchHost.exe" -
ServerName:MiniSearchUI.AppXj3y73at8fy1htwztzxs68sxx1v7cksp7.mca
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-handle=6632,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=6184 /prefetch:14
```

C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE

```
"C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE"
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --disable-gpu-sandbox --use-gl=disabled --gpu-vendor-id=4318 --gpu-device-id=140 --gpu-sub-system-id=0 --gpu-revision=0 --gpu-driver-version=10.0.22000.1 --string-annotations --gpu-preferences=UAAAAAAAAADoAAAEAAAAAAAAAAAAAAAAAAAABgAAEAAAAAAAAAAAAAAAAAAABCAAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAAEAAAAAAAAAAIAAAAAAAAAAgAAAAAAAAA --always-read-main-dll --field-trial-handle=3524,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=6552 /prefetch:10
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=unzip.mojom.Unzipper --lang=en-US --service-sandbox-type=service --video-capture-use-gpu-memory-buffer --string-annotations --always-read-main-dll --field-trial-handle=5324,i,7077681394194940702,18240694538911135317,262144 --variations-seed-version --mojo-platform-channel-handle=5212 /prefetch:14
```

5. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.28.11:80	edge.microsoft.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	api.edgeoffer.microsoft.com	udp
US	8.8.8.8:53	api.edgeoffer.microsoft.com	udp
US	8.8.8.8:53	copilot.microsoft.com	udp
US	8.8.8.8:53	copilot.microsoft.com	udp
US	13.107.213.64:443	api.edgeoffer.microsoft.com	tcp
GB	92.123.128.154:443	copilot.microsoft.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	update.googleapis.com	udp
US	8.8.8.8:53	update.googleapis.com	udp
GB	92.123.128.156:443	www.bing.com	tcp
GB	142.250.151.94:443	update.googleapis.com	tcp
US	8.8.8.8:53	clients2.googleusercontent.com	udp
US	8.8.8.8:53	clients2.googleusercontent.com	udp
GB	92.123.128.156:443	www.bing.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
GB	142.251.29.132:443	clients2.googleusercontent.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	edgeassetservice.azureedge.net	udp
US	8.8.8.8:53	edgeassetservice.azureedge.net	udp
US	13.107.213.64:443	edgeassetservice.azureedge.net	tcp
N/A	224.0.0.251:5353		udp
US	8.8.8.8:53	edge-consumer-static.azureedge.net	udp
US	8.8.8.8:53	edge-consumer-static.azureedge.net	udp
US	13.107.213.64:443	edge-consumer-static.azureedge.net	tcp
US	8.8.8.8:53	static.edge.microsoftapp.net	udp
US	8.8.8.8:53	static.edge.microsoftapp.net	udp
US	13.107.246.64:443	static.edge.microsoftapp.net	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
NL	93.123.17.252:80	msedge.b.tlu.dl.delivery.mp.microsoft.com	tcp
GB	92.123.128.192:443	www.bing.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
GB	2.16.153.207:443		tcp
AU	40.79.167.8:443	browser.pipe.aria.microsoft.com	tcp
IE	52.109.76.243:443	roaming.svc.cloud.microsoft	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp

GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
GB	52.109.28.48:443	odc.officeapps.live.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp

5. 6. Files

memory/3812-0-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3812-3-0x00007FFD05444000-0x00007FFD05445000-memory.dmp

memory/3812-2-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3812-1-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3812-6-0x00007FFD053A0000-0x00007FFD055A9000-memory.dmp

memory/3812-4-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3812-5-0x00007FFD053A0000-0x00007FFD055A9000-memory.dmp

memory/3812-7-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3812-8-0x00007FFD053A0000-0x00007FFD055A9000-memory.dmp

memory/3812-9-0x00007FFD053A0000-0x00007FFD055A9000-memory.dmp

memory/3812-10-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3812-11-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3812-12-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3812-14-0x00007FFD053A0000-0x00007FFD055A9000-memory.dmp

memory/3812-13-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

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

```
MD5     1427b17feb4de9e5ae0319bcd7d4c7e1
SHA1    491052eb95f524b764d30fbfb9950865a9bcdcfa
SHA256  6d4b6ee1d0c5a9cf4e947a884ecbbf3a2bf01ba9b3792585bbedf4ac9c587b47
SHA512  547e6d8ddcd105c1f2d0ec587a91fcc188b33650e912af1ff3c17995f7ae3165402c604ae5b685d88f9077bdac31eb9084e35757e8907b2523f365b219b63403
```

\??\pipe\crashpad_3040_UXFAVCPOARWMJIJZ

```
MD5     d41d8cd98f00b204e9800998ecf8427e
SHA1    da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA256  e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA512  cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e
```

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

```
MD5     59fd7eac1c7a5c24f54a0438f35677cb
SHA1    05c1c10e3fe316f0dafc7c714e3e7d05ae5e90f8
SHA256  c0e5b1b9820a8a674b49dc40a370b97d63612dd1f48fa2ba322b472520a1283c
SHA512  899075a77f5d203ec5768d4d4be0d8f2cf79498b29391329cd4e50b9eea0c473b44ef2ca8f67d4022dc229b4d900a65e7e1c9aba56840187b100d0022daaf1bb
```

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

```
MD5     41101bab6ae30fbf1307fbc2c455a3f2
SHA1    81d3d478ac338cb79b03db063a62f4027233d17b
SHA256  edafd9416105882e298dd1d5244cbcd7ffac584d36e85ee8f4a6400b0372ac0c
SHA512  bf2e6b60f7f378ec0c1c74920a33d880bc56cb71db942ab28b7ea310ecc8b3620e44f00a5aa839fd6547307c571b9288cadabf2c5e05633c0b049e7d2a3f5c69
```

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Network\SCT Auditing Pending Reports

MD5	d751713988987e9331980363e24189ce
SHA1	97d170e1550eee4afc0af065b78cda302a97674c
SHA256	4f53cda18c2baa0c0354bb5f9a3ecbe5ed12ab4d8e11ba873c2f11161202b945
SHA512	b25b294cb4deb69ea00a4c3cf3113904801b6015e5956bd019a8570b1fe1d6040e944ef3cdee16d0a46503ca6e659a25f21cf9ceddc13f352a3c98138c15d6af

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

MD5	b97d07c37ab0f523f291406453ddcd5c
SHA1	eb7f3f5dac005f17d7ac5458f2719441d3a87530
SHA256	38d992c285d186f414f698b1546378dc2a80ad8b1e6d1b0b9f6a9983f6de9ccf
SHA512	d771d5c56ccaaf5a2189b53f52a50cbac99914732415c5cc57de28efefc393858a8217132dee3a5a8ebcfa0a46810ab4cd906fe31115c02bc1f1c8fe7e77d8ae

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\DualEngine\SiteList-Enterprise.json

MD5	99914b932bd37a50b983c5e7c90ae93b
SHA1	bf21a9e8fbc5a3846fb05b4fa0859e0917b2202f
SHA256	44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
SHA512	27c74670adb75075fad058d5ceaf7b20c4e7786c83bae8a32f626f9782af34c9a33c2046ef60fd2a7878d378e29fec851806bbd9a67878f3a9f1cda4830763fd

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

MD5	3692b82273b09514a7212381ba0e0098
SHA1	5abf2cbf0bfd404c62a99944e2653830865eb23b
SHA256	a5f47979e3d9dc7c49694d8e9e4dd8e98b45470f93161940daff0b96bfc84a91
SHA512	d3611f1b0d1c4740eef4bb7d25dffc69de0afabb5f62164acb0d7e947175822cffdadfd607249028c6c6f9f39486e0e7dec0368f225793245ee820f59dcac4d7

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\CURRENT

MD5	46295cac801e5d4857d09837238a6394
SHA1	44e0fa1b517dbf802b18faf0785eeea6ac51594b
SHA256	0f1bad70c7bd1e0a69562853ec529355462fcd0423263a3d39d6d0d70b780443
SHA512	8969402593f927350e2ceb4b5bc2a277f3754697c1961e3d6237da322257fbab42909e1a742e22223447f3a4805f8d8ef525432a7c3515a549e984d3eff72b23

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Sync App Settings\ahokoikenoafgppiblgpenaaaolecifn\MANIFEST-000001

MD5	5af87dfd673ba2115e2fcf5cfdb727ab
SHA1	d5b5bbf396dc291274584ef71f444f420b6056f1
SHA256	f9d31b278e215eb0d0e9cd709edfa037e828f36214ab7906f612160fead4b2b4
SHA512	de34583a7dbafe4dd0dc0601e8f6906b9bc6a00c56c9323561204f77abbc0dc9007c480ffe4092ff2f194d54616caf50aecbd4a1e9583cae0c76ad6dd7c2375b

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

MD5	1fcc5330518c24dfd29bb2ce1378ae0d
SHA1	9a693b30dc884792ba5468fcfd31b7f1078ab20e
SHA256	f368187d6692608ba869583e2561e62b8b5872da7028ddc9b11714cc6ecd5b20
SHA512	6524436c91c8ef3443cc33763e602a7635f94dbdc6fb99db22d40a49fbf6da90176593974275b7a3788274e534dc91c7f0596bcc23fef62f5fcf6885b244de31

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Ad Blocking\blocklist

MD5	482ccb45b7248384e423f53f8539e192
SHA1	4ee5daf8b9be44f7327aa6c2e4fd0ae3158e5c5a
SHA256	4c0ef31a72bd5d02360216b0c5f9ae62422c17e378ca466e09077bd4b885bb78
SHA512	feeac04df4b0f4bf8bcb84286a6764943cfaa9a1013e10082c9768b9f2fc51d9ed82a070878947551825c572f5f9e18a646dc06c3282e027df4093b64d31d5b9

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\extensions_crx_cache\ghbmnnjooekpmoecnnnilnnbdlolhkhi_1.23b8196b76670ffac8063a91542118344bda24d7b2fa4a4c0dd146c4ee6b31b9

MD5	d6a332ceaa785f20d7cf0ef7b9fc4790
SHA1	65f275d0b2d7b017fc8727298498dd43833d0940
SHA256	23b8196b76670ffac8063a91542118344bda24d7b2fa4a4c0dd146c4ee6b31b9
SHA512	d79eba8bc96fe187f1284e7c3adf9323bd0525f73daba3e6f97013297588119256aa1af82ddccbdff5483b466f22b1846ee2f44afeb84fecd7f2c6951b7aa659

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

MD5	30fb8a7345bf814aabdfcba4b8ebc4e4
SHA1	421a8441e2d044808acc65eb4e58918dc7611a06
SHA256	fff60ea5e729e9d45b1f1fa5a2c13659009182163781920b0291032d2ac421fa
SHA512	8167b51697856e4792e62e1ed3384f88d897801f9a89f9ff7333f77f729493569237c84e22f0adcee0377054e713aab6867b12361cb301beb57a5d5cbb82638a

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

MD5	dd4df27c31575d7f10a7141f9e103dce
SHA1	5b0e1511e19cfa88a74d287bf1d79b36cf64aa08
SHA256	d01bb119fbec53224f174360a64be71010b9eed203d1bf58678f231bd6baa727
SHA512	c174f15bed85360ec477fd9ae09b7297578ec87362330e49623391c229f5f78f703e9025f22f040c45a99baae4b2339b56f6888ec372e0072ceb9be36a9931ef

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

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

memory/5260-421-0x0000012600000000-0x0000012601000000-memory.dmp

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

MD5	e7430f32fede83fdbb509483161a3154
SHA1	ac64b09b989420b8ccba943957283398e020a196
SHA256	04b2024f96a177214f59e61b0aba810a67fbf43e26560d9b7520476379d1d356
SHA512	33ad0baeab359f0466fec27d4417245e42c53fdab145dd250d89f46b1afb62387355cc2b0debd284f983caae4c4dedf1c4aa67b83368576e64c175ad3bc94803

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Edge Cloud Config\CloudConfigLog

MD5	a341a020a152490d5831a4d81fe9de80
SHA1	3ba9d2662e76c15f0c2664bc2887c835277b056b
SHA256	d84419115d013b4d50b151ea7f33c6e75b3b7c575473ea6b237b59fb62baec3f
SHA512	a6effd223f2e35b7638690e121ea0c96d121bfb740af2bc02893d301d14e99c96b0a9dacf536273f7836502c64335dcc53146df6fda7244c5f447bea00f3c008

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

MD5	f72cd300c5c33b75a81f4046f4d59bd5
SHA1	1b0bf5a6734e01a3514c0b98ed2d9c0b5c8961ae
SHA256	d9375969031463bdf7d041454b1b5ae5512ab0bf0a999920d6f6553503e37a26
SHA512	7773cff1f097558d92b9708cc68f9ce887f623fa2452678b85f562ac3871a73e2ebdf2105a7b6f64c018f7f2eb9dc288a04be2019561da5cafe7d086c0cf6a13

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

MD5	0b3db567fdba14f1dc57ac0a20da1ddc
SHA1	fab039dd4b37f651141c441e5c662b2b6bcba2bd
SHA256	19670a747da6e8936fba7d5ce0699460f1908cfc11d7760fb653f26966eed1de
SHA512	c82e326930b88a5dc1b9bf9ba5023ceda43e779da98cb5f6e8e88e4a0876149efd8213ff969264480ccefcdadc449ba7d7bf38e28981ae691e8ac7808fb19429

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1145337351\LICENSE

MD5	ee002cb9e51bb8dfa89640a406a1090a
SHA1	49ee3ad535947d8821ffdeb67ffc9bc37d1ebbb2
SHA256	3dbd2c90050b652d63656481c3e5871c52261575292db77d4ea63419f187a55b
SHA512	d1fdcc436b8ca8c68d4dc7077f84f803a535bf2ce31d9eb5d0c466b62d6567b2c59974995060403ed757e92245db07e70c6bddbf1c3519fed300cc5b9bf9177c

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1145337351\manifest.json

MD5	8ce95626b39ebc2401eee0b34c24fc7c
SHA1	f97a2fefe756f7a03e388e1333573b884730c2b0
SHA256	2d905d7b28b1afd313753d14f6a916a2e56ec4c1316bfa43046b09214ceb6090
SHA512	f04e4f695977918adf6e0603386b6f9c75a4a2202b0fe7215b642f3db491a1db398039cc28633b8e2541749403581622d28c1400f3f8fc66a3daab200e27266d

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

MD5	05523dac0edee8c94eb2b413b71a992b
SHA1	c59611b6bc945bf1565d8ef5a9a374dc8ebdd5b0
SHA256	68b9504d3429bd26574734b96810cf1f6dffac40c94f3953791f7abea730f4ab
SHA512	9d8a6031e0399dd16d3155cc599ddc37fda8f62e16655756578ce06241f7581fd23ed7ddb8fe37920f4cc2eca54fc0c155375453468cdd29bd143f8a33e318be

memory/3956-537-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3956-538-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3956-540-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3956-539-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3956-541-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3956-542-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3956-543-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3956-545-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/3956-544-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

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

MD5	6f963e343dac6a6e90cb79c28bd4d94f
SHA1	fa5cf38f14e9097769d8884899bd4dd434be5b00
SHA256	625592fc66f5f13fe257a2915e168b184b2d7ef0ee5de9af21377428e57e885f
SHA512	fd3fcae04d1320457f26d4aa7781ef4b8c04f49ed52edd17393b1c6f6ec7b3beeb976cc6d62438eb31371f4260245cf73bdaac32713da26ee61b1e2b0dc7a712

C:\Users\Admin\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TempState\SearchHoverUnifiedTileModelCache.dat

MD5	aaaca500411a3ce3c55b3c3c3947a91b
SHA1	bd5331039190a1b0e0269bc26e5b4cf8c0987f8b
SHA256	c949d1f02630fb8bd979377309fc55316276d49fd0cbcdefb0fd5210bac44d25
SHA512	b219c8682935970f1b83b0e684e8bfcdf54e9cc469e2c37748a5e809d8aad4fd71f9645b53d984b97a5612e21072164b6baf2317769ea6adb8d7e9f3359b79a8

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_1919145674\manifest.json

MD5	0726a393d6366788cb47da5897d1af64
SHA1	022ebd4d118261b871d50479868d502b797e6d14
SHA256	7c00a941d7a04048f469ffb986ff7e8bf349f149639cc474a463da4a607c0a70
SHA512	adaaf0c40793c606d44fd7112b42040f01dd483a7c4c678e811f824e2fbad722ee3faf50984615731d71425eb3a1e4a9090962249e673fe8e7290713c8f75d9f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\TrustTokenKeyCommitments\2025.9.29.1\keys.json

MD5	80068ae175438916aff814972b76e6f6
SHA1	39336911d02ae3c5b038aa31c73c4757dcfadab6
SHA256	e5b57a8978e405e9487c43e6b0b3685c4c71cdaa2e74e25d7fbed75ffaea01b2
SHA512	7cd55dc8c37fbaf9675d08fd2346ee45721338e1e70cf6aa351e54b45630ada5ada1243d738742cbda258c830e25ee8e09f57fc3cf21948e62c3c552ba9cd18d

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

MD5	aacf33f4e89ec99b4436895e9c8a4878
SHA1	3f194c6a02ff828285edb4bf38dfeca7ff3ec2df
SHA256	ab451f6f5a137251e2cd58a138fbc75b85da7d6a1f42b5f9153d3431b380f967
SHA512	d77f0798dd11b28db6f5f9726c0f2cc3b3cb959209ca85aab217425cb5c3857953e082f057051889757012b56c838c1339f111c9f4302b96b3a97413c3fab9eb

memory/640-601-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/640-603-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/640-611-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/640-604-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/640-602-0x00007FFCC5430000-0x00007FFCC5440000-memory.dmp

memory/640-614-0x00007FFCC29B0000-0x00007FFCC29C0000-memory.dmp

memory/640-615-0x00007FFCC29B0000-0x00007FFCC29C0000-memory.dmp

C:\Users\Admin\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\odc.officeapps.live.com\E1E3D242-C8F8-459F-B445-33153262DED2

MD5	2f82426450332b558a61ae9ca551abd9
SHA1	abdbf8f8bdd7572bcdefbd1e0b7da8d3cf17144d
SHA256	57d6315a8f1f11aaa111a9956ddd0d560f791f757c379ed77bbb5a1b5b577f52
SHA512	dbc43dab6cbde98647c5a88cd508a1528ef79c030286cf82cb4cb03c4af81930ad1c3b2644ead9eceea27cd5772324f42a51f04f1693102254567205a6abf0b5

C:\Users\Admin\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\odc.officeapps.live.com\B278E7AA-C67E-456F-8741-FF195AED58CE

MD5	85ad173999ed440af6120f3b4fd436fa
SHA1	eebe3bae40b0c82db581b905e2a4c4a90055c9b3
SHA256	2fb3e7ca57b5ec8657ff2b909c74dee246e7ed2b30abd60dec96fc4fb88bd165
SHA512	3c506252a27bc4a3d718fc2ad89036850ee3c9d5fd79966fc5e28debe1844d96e8d2777e160e8537034129fd8109dff027bf5eb4a082c99d0db93730ec31427e

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\b8ab77100df80ab2.customDestinations-ms

MD5	708831f3a0b6c5e6fb37eacca6e98796
SHA1	fbcef7ada666a6bb42506970b5b35507562829d3
SHA256	c27b40ba878f8c92f0c67e967e75bbc761372ee95d28afdfc66b40ff9e9af92e
SHA512	eefbf39e6ae403a49d3008804f2a95cbeddf1447b62e448430e282393f12265c1bd23bce26d6ceb848f912648abf99480592a337e8d9250c00e648e22691e876

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

MD5	0847880286128db559f5ed7cb2b2fdad
SHA1	af16bd58d680811b8f78eb37630ee29ff1f0a175
SHA256	cbfb3585e0d339beb2752bfe8126130bb8078463f5c0c696568d8985eb128763
SHA512	789edabd8176e1a93865883e18e059e247a76f7e661e6c9cd57444f292e36bf731ac35794451ffb553fb55d0cc949253c735e47f552fbbc560f326d366160913

C:\Windows\SystemTemp\chrome_Unpacker_BeginUnzipping3040_409228308\manifest.json

MD5	f99766abe08dd2f4607288031ffcb71d
SHA1	40f82d7a810175043004f10366a763180f4cbe13
SHA256	cd3bfb95cabb4cce04ae822443c4e7ef5c16ef8364804b3907bf37775f821eac
SHA512	a6cde975e71a816377c2837d0941b0c7e68d730dec93d157b4171839e6a0314fb599053111b2e1951b0b90b23ae5cd06e23e7b7cbd01d6f9a6928cad82bf5e17