Recorded Future® Sandbox

Malware Analysis Report

2025-12-27 22:54

Sample ID	251227-2k5bys1jhv
Target	Radar_Inwestora_v4_3 (2).exe
SHA256	0acccbe10f53b441a6f170e8b7c17638ce46c323bf759c582679cba9ed1fb697
Tags	pyinstaller discovery execution phishing

score

7/10

Table of Contents

Part 1. Analysis Overview

score

7/10

SHA256
0acccbe10f53b441a6f170e8b7c17638ce46c323bf759c582679cba9ed1fb697

Threat Level: Shows suspicious behavior

The file Radar_Inwestora_v4_3 (2).exe was found to be: Shows suspicious behavior.

Malicious Activity Summary

pyinstaller discovery execution phishing

- **Loads dropped DLL**
- **A potential corporate email address has been identified in the URL: **
- **Command and Scripting Interpreter: PowerShell**
- **Detects Pyinstaller**
- **Enumerates physical storage devices**
- **System Time Discovery**
- **Browser Information Discovery**
- **Unsigned PE**
- **Suspicious use of FindShellTrayWindow**
- **Modifies registry class**
- **Modifies data under HKEY_USERS**
- **Suspicious behavior: EnumeratesProcesses**
- **Suspicious use of WriteProcessMemory**
- **Suspicious use of AdjustPrivilegeToken**
- **Enumerates system info in registry**
- **Suspicious behavior: NtCreateUserProcessBlockNonMicrosoftBinary**
- **Checks processor information in registry**

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Reconnaissance TA0043			
Resource Development TA0042			
Initial Access TA0001			
Execution **TA0002**	Command and Scripting In… T1059		
	PowerShell T1059.001		
Persistence TA0003			
Privilege Escalation TA0004			
Defense Evasion TA0005			
Credential Access TA0006			
Discovery **TA0007**	Browser Information Disco… T1217	Query Registry T1012	System Information Disco… T1082
	System Time Discovery T1124		
Lateral Movement TA0008			
Collection TA0009			
Command and Control TA0011			
Exfiltration TA0010			
Impact TA0040			

Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-12-27 22:39

3. 2. Signatures

Detects Pyinstaller

pyinstaller

Description	Indicator	Process	Target
N/A	N/A	N/A	N/A

Unsigned PE

Description	Indicator	Process	Target
N/A	N/A	N/A	N/A

Part 4. Analysis: behavioral2

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-12-27 22:39	2025-12-27 22:48	win11-20251223-en	150s	95s

4. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe"
```

4. 3. Signatures

Loads dropped DLL

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A

Suspicious use of WriteProcessMemory

Description	Indicator	Process	Target
PID 3472 wrote to memory of 3416	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe

4. 4. Processes

C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe
"C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe"

C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe
"C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe"

4. 5. Network

4. 6. Files

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Africa\Conakry

MD5	09a9397080948b96d97819d636775e33
SHA1	5cc9b028b5bd2222200e20091a18868ea62c4f18
SHA256	d2efac4e5f23d88c95d72c1db42807170f52f43dd98a205af5a92a91b9f2d997
SHA512	2eccf2515599ed261e96da3fbcfbab0b6a2dfc86a1d87e3814091709f0bfe2f600c3044c8555ed027978a8ae9045666ee639a8c249f48d665d8e5c60f0597799

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Africa\Djibouti

MD5	86dcc322e421bc8bdd14925e9d61cd6c
SHA1	289d1fb5a419107bc1d23a84a9e06ad3f9ee8403
SHA256	c89b2e253a8926a6cecf7eff34e4bfcdb7fe24daff22d84718c30deec0ea4968
SHA512	d32771be8629fb3186723c8971f06c3803d31389438b29bf6baa958b3f9db9a38971019583ba272c7a8f5eb4a633dfc467bfcb6f76faa8e290bad4fd7366bb2b

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Africa\Kigali

MD5	b07064beada5be6289ed9485ecc9733d
SHA1	b0ff96d087e4c86adb55b851c0d3800dfbb05e9a
SHA256	444ed3a710414bc6bf43eb27e591da49d3be3db153449a6a0c9473f7e39fdbcb
SHA512	0ce1322f4a6f6568cdf61fc699eead4147015829650e90d791c223b45f3a23ead720ff41b4c8cc10ee915175e052d4740347a4454d23c18a3c57d30ded5a904c

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Africa\Lagos

MD5	8244c4cc8508425b6612fa24df71e603
SHA1	30ba925b4670235915dddfa1dd824dd9d7295eac
SHA256	cffeb0282ccbd7fba0e493ff8677a1e5a6dd5197885042e437f95a773f844846
SHA512	560c7581dcb2c800eae779005e41406beaf15d24efc763304e3111b9bb6074fe0ba59c48b5a2c5511245551b94418bbc35934d9bd46313fcc6e383323056668c

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\America\Curacao

MD5	adf95d436701b9774205f9315ec6e4a4
SHA1	fcf8be5296496a5dd3a7a97ed331b0bb5c861450
SHA256	8491e557ff801a8306516b8ca5946ff5f2e6821af31477eb47d7d191cc5a6497
SHA512	f8fceff3c346224d693315af1ab12433eb046415200abaa6cdd65fd0ad40673fdddf67b83563d351e4aa520565881a4226fb37d578d3ba88a135e596ebb9b348

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\America\Toronto

MD5	8dabdbbb4e33dcb0683c8a2db78fedc4
SHA1	a6d038ecff7126ee19ebb08a40d157c9a79964cd
SHA256	a587a1a1607439f7bac283e1815f2bdbafb9649a453d18e06c2e44e6996d888f
SHA512	35bfd5182535f5257d7ee693eb6827751993915129d7f3cc276783926b1f4db7a00d8f0b44a95ac80c294a9cc1b84bda6418134c2a5c10ba6c89946bd8ef97a3

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\EST

MD5	0972a9c4c28bf71eeab5f0bac573cdbc
SHA1	a94fbc2d567e41723f03629b6c9a864260108a17
SHA256	91ac80fe976931c490d058c8ce8b5d71ffa6d4961f6ca13ea9c153f0b0bccea0
SHA512	ece548f7d840a588523aacddc93891e0dd300390f79de063e60074e00a92ae33a8201642b841ff868387f1ac2188c485cce941d83c7a3617d27ac286dbcc0c17

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Etc\Greenwich

MD5	9cd2aef183c064f630dfcf6018551374
SHA1	2a8483df5c2809f1dfe0c595102c474874338379
SHA256	6d9f378883c079f86c0387a5547a92c449869d806e07de10084ab04f0249018d
SHA512	dafa0cb9d0a8e0ff75a19be499751ad85372aafa856ff06dd68ecf2b1c5578bb98a040becaecf0aed2c3e4ff7372ff200fe7614334756d19fe79dd61c01d4e92

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Europe\London

MD5	a40006ee580ef0a4b6a7b925fee2e11f
SHA1	1beba7108ea93c7111dabc9d7f4e4bfdea383992
SHA256	c85495070dca42687df6a1c3ee780a27cbcb82f1844750ea6f642833a44d29b4
SHA512	316ecacc34136294ce11dcb6d0f292570ad0515f799fd59fbff5e7121799860b1347d802b6439a291f029573a3715e043009e2c1d5275f38957be9e04f92e62e

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Europe\Oslo

MD5	7db6c3e5031eaf69e6d1e5583ab2e870
SHA1	918341ad71f9d3acd28997326e42d5b00fba41e0
SHA256	5ee475f71a0fc1a32faeb849f8c39c6e7aa66d6d41ec742b97b3a7436b3b0701
SHA512	688eaa6d3001192addaa49d4e15f57aa59f3dd9dc511c063aa2687f36ffd28ffef01d937547926be6477bba8352a8006e8295ee77690be935f76d977c3ea12fe

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Europe\Skopje

MD5	6213fc0a706f93af6ff6a831fecbc095
SHA1	961a2223fd1573ab344930109fbd905336175c5f
SHA256	3a95adb06156044fd2fa662841c0268c2b5af47c1b19000d9d299563d387093a
SHA512	8149de3fd09f8e0f5a388f546ffe8823bdcda662d3e285b5cebc92738f0c6548ccb6ed2a5d086fd738cb3edc8e9e1f81c5e2e48edb0571e7ea7f131675b99327

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\PRC

MD5	09dd479d2f22832ce98c27c4db7ab97c
SHA1	79360e38e040eaa15b6e880296c1d1531f537b6f
SHA256	64ffc2e43a94435a043c040d1d3af7e92d031adc78e7737af1861baa4eeef3e6
SHA512	f88ae25f3f04c7d5d5f98aafecc03cc7e4e56f1cd4c8deba6afd043f0fb7fe67b4d50e4df5493e77c6b34ba183e019442e736a13f784ba8c2847c06fd74ff200

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\MET

MD5	355f0d3e2a3ee15ea78526f5eeb0cf7d
SHA1	d90f3247c4716c2e1068d5ad9c88ca2091bec4e8
SHA256	812f55aeb6e8cde9ddf4786e15eb4256b21e82cf5f5d28da1bad17d94570cac0
SHA512	96a5fa48a15167e55ffad5b0241c90caeb7f0433ad62dd43463a4c52c25c59f7357681cb586fc52e812e8173adc12cec9eff66d27d5f41e19d55f6c1fce12937

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\US\Mountain

MD5	648f67a7744849f2ca07f4d5871e9021
SHA1	faa7d6cf4178d032d8ba8a4d77eac0fd47f8a718
SHA256	32e819c00a43b3c348f539d700d425504f20b8d068c16418d26fa9b693e775c9
SHA512	3dab6d6a04a4856cba78ef499f1a436f1f71b1dea494ee098b76c1702531108ae0a1d7b6de05e9d9315027624b790e084d69b25507738099f6026cd2a9559f31

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\UCT

MD5	38bb24ba4d742dd6f50c1cba29cd966a
SHA1	d0b8991654116e9395714102c41d858c1454b3bd
SHA256	8b85846791ab2c8a5463c83a5be3c043e2570d7448434d41398969ed47e3e6f2
SHA512	194867d0cf66c2de4969dbfeb58c775964ecb2132acdc1b000b5ef0998cefde4a2979ffc04ec8b7dcb430e43326a79d9cedb28ecea184345aa7d742eaf9234ac

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Pacific\Yap

MD5	ec972f59902432836f93737f75c5116f
SHA1	331542d6faf6ab15ffd364d57fbaa62629b52b94
SHA256	9c1dfa1c15994dd8774e53f40cb14dcf529143468721f1dba7b2c2e14ae9f5f0
SHA512	e8e8c8f6d096c352d1244280254e4c6ecf93f7c2ff69ecc6fa4363a6be8a2daf6cfcd7f0d96bc2669268ced5565532fa06be348a139b0742ccccb83953c6324d

C:\Users\Admin\AppData\Local\Temp_MEI34722\pytz\zoneinfo\Pacific\Wallis

MD5	5bdd7374e21e3df324a5b3d178179715
SHA1	244ed7d52bc39d915e1f860727ecfe3f4b1ae121
SHA256	53268a8a6b11f0b8e02fc67683ae48d074efaf7b4c66e036c1478107afd9a7d7
SHA512	9c76f39e8795c50e6c5b384a7ff1f308a1c5173f42f810759b36cdeae7d33d1dac4934efeed580c59d988c152e2d7f8d9b8eb2073ab1fc15e4b9c10900c7b383

C:\Users\Admin\AppData\Local\Temp_MEI34722\ucrtbase.dll

MD5	286b308df8012a5dfc4276fb16dd9ccc
SHA1	8ae9df813b281c2bd7a81de1e4e9cef8934a9120
SHA256	2e5fb14b7bf8540278f3614a12f0226e56a7cc9e64b81cbd976c6fcf2f71cbfb
SHA512	24166cc1477cde129a9ab5b71075a6d935eb6eebcae9b39c0a106c5394ded31af3d93f6dea147120243f7790d0a0c625a690fd76177dddab2d2685105c3eb7b2

C:\Users\Admin\AppData\Local\Temp_MEI34722\python311.dll

MD5	387bb2c1e40bde1517f06b46313766be
SHA1	601f83ef61c7699652dec17edd5a45d6c20786c4
SHA256	0817a2a657a24c0d5fbb60df56960f42fc66b3039d522ec952dab83e2d869364
SHA512	521cde6eaa5d4a2e0ef6bbfdea50b00750ae022c1c7bd66b20654c035552b49c9d2fac18ef503bbd136a7a307bdeb97f759d45c25228a0bf0c37739b6e897bad

C:\Users\Admin\AppData\Local\Temp_MEI34722\libffi-8.dll

MD5	0f8e4992ca92baaf54cc0b43aaccce21
SHA1	c7300975df267b1d6adcbac0ac93fd7b1ab49bd2
SHA256	eff52743773eb550fcc6ce3efc37c85724502233b6b002a35496d828bd7b280a
SHA512	6e1b223462dc124279bfca74fd2c66fe18b368ffbca540c84e82e0f5bcbea0e10cc243975574fa95ace437b9d8b03a446ed5ee0c9b1b094147cefaf704dfe978

C:\Users\Admin\AppData\Local\Temp_MEI34722_ctypes.pyd

MD5	565d011ce1cee4d48e722c7421300090
SHA1	9dc300e04e5e0075de4c0205be2e8aae2064ae19
SHA256	c148292328f0aab7863af82f54f613961e7cb95b7215f7a81cafaf45bd4c42b7
SHA512	5af370884b5f82903fd93b566791a22e5b0cded7f743e6524880ea0c41ee73037b71df0be9f07d3224c733b076bec3be756e7e77f9e7ed5c2dd9505f35b0e4f5

C:\Users\Admin\AppData\Local\Temp_MEI34722\python3.dll

MD5	7e07c63636a01df77cd31cfca9a5c745
SHA1	593765bc1729fdca66dd45bbb6ea9fcd882f42a6
SHA256	db84bc052cfb121fe4db36242ba5f1d2c031b600ef5d8d752cf25b7c02b6bac6
SHA512	8c538625be972481c495c7271398993cfe188e2f0a71d38fb51eb18b62467205fe3944def156d0ff09a145670af375d2fc974c6b18313fa275ce6b420decc729

C:\Users\Admin\AppData\Local\Temp_MEI34722\base_library.zip

MD5	99ada859f99e907452d98b7911f3cf34
SHA1	a23d5e35eb36ab369dc4b2ebf0ea263e1014e93a
SHA256	2b573c891e17cc325aa944d67d7d020ac32dfb58400c256dbd4fe61e2bde8c59
SHA512	5ebd57e9305463f95046ca2dd5dc71155331fa026cd648a7f9b6c51938ee6ed4b8080bbe24c5a08dfbd75269962da0dc3111698b7f6eebb876e51a3b709f2e87

C:\Users\Admin\AppData\Local\Temp_MEI34722\VCRUNTIME140.dll

MD5	be8dbe2dc77ebe7f88f910c61aec691a
SHA1	a19f08bb2b1c1de5bb61daf9f2304531321e0e40
SHA256	4d292623516f65c80482081e62d5dadb759dc16e851de5db24c3cbb57b87db83
SHA512	0da644472b374f1da449a06623983d0477405b5229e386accadb154b43b8b083ee89f07c3f04d2c0c7501ead99ad95aecaa5873ff34c5eeb833285b598d5a655

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-processthreads-l1-1-1.dll

MD5	385f562bdc391ccd4f81aca3719f3236
SHA1	f6633e1dac227ba3cd14d004748ef0c1c4135e67
SHA256	4ad565a8ba3ef0ea8ab87221ad11f83ee0bc844ce236607958406663b407333e
SHA512	b72ed1a02d4a02791ca5490b35f7e2cb6cb988e4899eda78134a34fb28964ea573d3289b69d5db1aac2289d1f24fd0a432b8187f7ae8147656d38691ae923f27

C:\Users\Admin\AppData\Local\Temp_MEI34722\tk86t.dll

MD5	50be514d4234103d49fb2a600a272fce
SHA1	e441b77a421598998d24814afd4af8090d306e57
SHA256	b6af038120f2b8644c7ce1e11917f410009848287622135d7e386f90d28a831c
SHA512	d93467b688f68f15eb46dc1aef4bd4f4d0b91193a2c40a1d4b5cc6e906a443343e261225df530527491a01c58803b91a138d5147d7a02aedeb9cddd3adc77fef

C:\Users\Admin\AppData\Local\Temp_MEI34722\select.pyd

MD5	e4ab524f78a4cf31099b43b35d2faec3
SHA1	a9702669ef49b3a043ca5550383826d075167291
SHA256	bae0974390945520eb99ab32486c6a964691f8f4a028ac408d98fa8fb0db7d90
SHA512	5fccfb3523c87ad5ab2cde4b9c104649c613388bc35b6561517ae573d3324f9191dd53c0f118b9808ba2907440cbc92aecfc77d0512ef81534e970118294cdee

C:\Users\Admin\AppData\Local\Temp_MEI34722\tcl86t.dll

MD5	50be441afc42714cb7fe98677f304807
SHA1	0604a2992f698e45d1524c44a924b7451d8ad003
SHA256	4e699ff2d6d147d0586c8c77be5a18f20ca0758f432d7b0f489223f2fa4dd221
SHA512	a99c7b5c9d42c53cf51ace16871bb2f1dfc9424077b0a758ec1b8583eb1be3cdd413d005188fa82dd61093b56882cd72b32f15b55599c5f0fcbce34321afb639

C:\Users\Admin\AppData\Local\Temp_MEI34722\sqlite3.dll

MD5	89c2845bd090082406649f337c0cca62
SHA1	956736454f9c9e1e3d629c87d2c330f0a4443ae9
SHA256	314bba62f4a1628b986afc94c09dc29cdaf08210eae469440fbf46bcdb86d3fd
SHA512	1c467a7a3d325f0febb0c6a7f8f7ce49e4f9e3c4514e613352ef7705a338be5e448c351a47da2fb80bf5fc3d37dbd69e31c935e7ff58ead06b2155a893728a82

C:\Users\Admin\AppData\Local\Temp_MEI34722\pyexpat.pyd

MD5	79561bc9f70383f8ae073802a321adfb
SHA1	5f378f47888e5092598c20c56827419d9f480fa7
SHA256	c7c7564f7f874fb660a46384980a2cf28bc3e245ca83628a197ccf861eab5560
SHA512	476c839f544b730c5b133e2ae08112144cac07b6dfb8332535058f5cbf54ce7ed4a72efb38e6d56007ae755694b05e81e247d0a10210c993376484a057f2217c

C:\Users\Admin\AppData\Local\Temp_MEI34722\libssl-3.dll

MD5	19a2aba25456181d5fb572d88ac0e73e
SHA1	656ca8cdfc9c3a6379536e2027e93408851483db
SHA256	2e9fbcd8f7fdc13a5179533239811456554f2b3aa2fb10e1b17be0df81c79006
SHA512	df17dc8a882363a6c5a1b78ba3cf448437d1118ccc4a6275cc7681551b13c1a4e0f94e30ffb94c3530b688b62bff1c03e57c2c185a7df2bf3e5737a06e114337

C:\Users\Admin\AppData\Local\Temp_MEI34722\libcrypto-3.dll

MD5	e547cf6d296a88f5b1c352c116df7c0c
SHA1	cafa14e0367f7c13ad140fd556f10f320a039783
SHA256	05fe080eab7fc535c51e10c1bd76a2f3e6217f9c91a25034774588881c3f99de
SHA512	9f42edf04c7af350a00fa4fdf92b8e2e6f47ab9d2d41491985b20cd0adde4f694253399f6a88f4bdd765c4f49792f25fb01e84ec03fd5d0be8bb61773d77d74d

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-utility-l1-1-0.dll

MD5	708a5bc205384633a7b6674eecc7f0f0
SHA1	01603a7826029293236c67fce02ace8d392a0514
SHA256	d8ba5f17b9ffcbf3aeaf3fa1da226832d2fa90f81acce0cd669464e76ce434ac
SHA512	8638845326ab6543338baa7a644af8be33a123e1fc9da2037158be7c8d165691ccd06cb3ff73696a30b8801eab030e81f93db81216bb3b7e83a320a0df5af270

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-time-l1-1-0.dll

MD5	fccce207a34c947f01d3f23a7dd09569
SHA1	75f722801c77285db98a08af763252a0255e99e2
SHA256	7c7f6393f06de11750adb09cc5698ae55cd9fb27b2e51e207286feb1b5b2b156
SHA512	d3d923f133594eb4325f4a6e5ed46fcc348a7c0f310f14eaa38c6fad070ba637bdb4a77200feb231114e111d07a86595a6130291028cde3a284d9f847ec38ad4

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-string-l1-1-0.dll

MD5	639b1fb35cb61ba633eb1791b750631f
SHA1	392a6925009f5fb02a4c122c9ce31d82b9059628
SHA256	25b8f83a7767211b11132775a0e27a45aa4ec8ab4e6572599f9c172ae3606b40
SHA512	def547ef66673862cea9bb13c433edce24a3075c328d9b3b9452f2f01f2f4243daab38c0f8571c52d601bc4aecaaa0682dbebf6be41cae345787a719063ebf58

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-stdio-l1-1-0.dll

MD5	ef37235fc43157a4c93241d5e49e304b
SHA1	d4de26b36812c2ddccd1618b4d7ac02ad1b42273
SHA256	a9c5a153d8c0286f9b41a2b1c65854ad9e6471b8755b7de87bae4470e60bcab6
SHA512	c0857760d5d069beeb1eb1737f4160530910331bf6047022836cf58137bd28c2a966a8760a681859f57ebd810fd424ce231402eddde1316eaef7b6f9f773afbb

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-runtime-l1-1-0.dll

MD5	bbaa58e9e1abdf7d8c4c69652d29d789
SHA1	38aef13abc14502354e8c5c3c37b97a8e2e5fdcf
SHA256	c5902934d026d7e15fbe9917d474f3322846a41a25e66f4b2b1f758801879f4b
SHA512	7882a8e1e1ea7e217f70ff9df27d36709b4be23588909ef002f3eb1b9a7d3eea2591a8524af2c83448ddfff0911658517c6989683245c54678583f359a78b0ad

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-process-l1-1-0.dll

MD5	9d6925407136753e8eb8234d59fa3f1f
SHA1	62631b7007d394fb4d406ea686b291fff9e486cd
SHA256	f6156b1020380ec4f0e48577ebedaaef5fb1ab1f337d8b4e72e6a33a7567a9cc
SHA512	ab04de62524e465810cd0ee81e85018863e276d49861e67a920667af802e94869b816b47a6e3c4738179a7a7d726d44bbba6e47d9097363a63eaff51cd56de8a

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-private-l1-1-0.dll

MD5	c830c6447e6de3d6a611702c591831e3
SHA1	2b5a0a8702c769eeaaf101852456aa3ecf3914e3
SHA256	1bc82bed6143d2bf1b6b08a7809f4a5e29317d6fddd338a7da3c0223522e4bbf
SHA512	9ad2b9fd4792632714394f0dc293776484d16b1efbaba2daf1816df911a58fe4a920c48059b44848681b7a266a0ea036ec36ee0a031f52c034a15ad74d3bdb51

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-math-l1-1-0.dll

MD5	aa9624cb27cc50a3fbbd3b223a617b1c
SHA1	797aea1c5cedd1125276bfc5dcd7a3fb8c6355aa
SHA256	606d66d82db562ea7979179d06486a0f94d079941d26b80a1e2c49d29959df6f
SHA512	024975e6787f7a6b0ab6e4b02ad33901f8473b97dc73d4f03b7a116b24ac74150c0c48990ea7a4fb750f9fe728dafed172796743f802e70f2150eefcf70fe96a

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-locale-l1-1-0.dll

MD5	09796dab12cbbd920f632aeb89820193
SHA1	7d81c0e5537b6d8b79af0c28cd102e064027c78d
SHA256	bd14c67ea28e21d6257ad780a37122c9b5773f69e693f5db6bffaee4d839526e
SHA512	09a6175dccbbd18a62209e156089f1167dfb8040c97c8c2c14724ce2a8fbe6ce039d7fe04fb8bd60092427beb7fdd8e7127d611f006fff1cf2a1ad75e9e5ef3a

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-heap-l1-1-0.dll

MD5	527bbbfded529ea77ee798d94ce0f243
SHA1	647f8c89eb4db3cf3656292b3de984b32c6e02a5
SHA256	bab9ac3ec83e380ae51e4295ef3bf2c738627812d3a49d1e713661abbc8dc57a
SHA512	c1ed69e15ab19084390cf9d1ceab791758ac4ddd688169f3b814b0e4cf1fc3b6ba17651e35b25dcdc601a8a64821d58933d52a5e939942fa134dfd04fca04c8b

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-filesystem-l1-1-0.dll

MD5	47555752931cecf90e796499b62ec729
SHA1	217b171764fba5e91190d1f8a36feccb3f6d4585
SHA256	9a9e2a65a281644e368d0f272b95ba5f6b445d1c35910d06056c5ebeb77402db
SHA512	a68009f0306d4d8e70951978d2c184eb80fbec98c6db0997bd7b0b503dd63019363cfef68a9adbfb568c0a552b774fbdbeb1bcf45f211a6a3224b49e85a5619c

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-environment-l1-1-0.dll

MD5	e93c7f013493b12ad40229b19db02ce6
SHA1	ef878bfbfd2f8328bbb8cff1aa29a39e624a8503
SHA256	17d63275d00bdd8670422b95bd264c532998e0a1b041079e54fce4b6b7a55819
SHA512	2f4a25ea4062840bea10442cad665a72abbce747307ad9ce7b3bb89eaf7dcc28f1e9396749576be304fd793690ddc4456536134404426695e72b761eacacb6020

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-convert-l1-1-0.dll

MD5	3560176d0cdbe2f5d33f543348e0a027
SHA1	1e35a1f7793fc3899927835491f28fe5b903edcd
SHA256	ebb2ae5535a64f65daeab8235585114fc9dd2cf1a49f5852d446250b998b6ae4
SHA512	8ab24c8c9fe8331f21be96818c5fa69ae5578eb742c4504596310bb0db7c4c087d350fa47a13ed9ff2e051bb62ac5581de082d0177923d24fee6b140afecf50b

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-crt-conio-l1-1-0.dll

MD5	5794b8e183eb547aadd5faf30a8c4dd2
SHA1	5b1ed8a9da14d8ecc4209662809727931aa49307
SHA256	b762061b688aae679afe788904d2c9970f74a7dac98f3b42463d08f25e483d3f
SHA512	3e896854e5dd957ab2b88c82fbaf2eaa03729bab30fd8518bd999081f4da9000d9b22894b324e5930df161c7adaec3fc87fd00de60dcda34876007aea4a2fd31

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-util-l1-1-0.dll

MD5	3c58a804b90a0782e80bbbf6c6b6f167
SHA1	b333143e0f6e508b51d27adf7872b586fa54c794
SHA256	6eda016742a6171205a387a14b3c0b3318415677403 76f56768f8c151724207d
SHA512	773f8deded48b34babe24d955a501f4f357c20125affb6eade36ce6a7acd380906713c366318f79d627747e636d156875c216fffac26dba25373bbc1c820da76

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-timezone-l1-1-0.dll

MD5	43d8d2fb8801c5bd90d9482ddf3ea356
SHA1	d582b55cd58531e726141c63ba9910ff185d72e0
SHA256	33f4fddc181066fce06b2227bded813f95e94ed1f3d785e982c6b6b56c510c57
SHA512	0e073381a340db3f95165dbcceb8dfbf1ed1b4343e860446032400a7b321b7922c42ee5d9a881e28e69a3f55d56d63663adb9bb5abb69c5306efbf116cc5e456

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-sysinfo-l1-2-0.dll

MD5	fc9fc5f308ffc2d2d71814df8e2ae107
SHA1	24d7477f2a7dc2610eb701ed683108cd57eca966
SHA256	2703635d835396afd0f138d7c73751afe7e33a24f4225d08c1690b0a371932c0
SHA512	490fa6dc846e11c94cfe2f80a781c1bd1943cddd861d8907de8f05d9dc7a6364a777c6988c58059e435ac7e5d523218a597b2e9c69c9c34c50d82cac4400fe01

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-sysinfo-l1-1-0.dll

MD5	b65bf5ef316880fd8d21e1b34eb5c8a9
SHA1	3ab4674cb5c76e261fe042d6d0da8a20bfcbcbae
SHA256	b203d862ddef1dd62bf623fc866c7f7a9c317c1c2ae30d1f52cb41f955b5698e
SHA512	4af3b0ef9a813ce1a93a35dd6869817910ae4b628f374477f60ea1831d2cc1aae7908262672e11954a4953bdff22bcc5fe23b4a736788e8e5ef4f8ac30eb24f8

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-synch-l1-2-0.dll

MD5	8f107a7bc018227b181a0e7e76e9ca39
SHA1	ef57e24f29d2b1deeacefd82171873b971a3f606
SHA256	efc1e4460984a73cf47a3def033af1c8f3b1dbc1a56cd27781d3aacf3e3330cb
SHA512	d8d8250aaf93fa99e9d1e4286b32579de0029c83867a787c0a765505a0f8cbd2dd076bb324509d5c4867423bc7dc8f00c8b8458e08e8cbfa8dd731d03dd1ae3f

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-synch-l1-1-0.dll

MD5	436ea0237ed040513ec887046418faaa
SHA1	44bafbbdb1b97d86505e16b8a5fcb42b2b771f91
SHA256	3a72b4f29f39a265d32ad12f0ce15dbf60129c840e10d84d427829ede45e78ad
SHA512	9f0dbfb538c05383ae9abfe95e55740530ecc12c1890d8862deacbc84212be0740d82afc9e81d529125221e00b2286cae0d4b3ca8dd3a6c57774d59f37933692

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-string-l1-1-0.dll

MD5	28005b20fbef6e1db10912d0fdd6471c
SHA1	47b83697677e08e4ebcff6fc41eca7ece120cc17
SHA256	60fc31d2a0c634412f529dba76af3b9bf991352877c6dae528186d3935704cfd
SHA512	45d6f860d7f7aefaa7a0a3b4b21b5c3234f442e39d6259e0a9e2083890533c275f07ddda93fddc7445928a55475b83c63253d3b08e41e5576f9029b205dfb36a

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-rtlsupport-l1-1-0.dll

MD5	3c5c7a3130b075b2def5c413c127173f
SHA1	f3d2b8ad93f3dc99c8410d34c871aec56c52e317
SHA256	9dc1e91e71c7c054854bd1487cb4e6946d82c9f463430f1c4e8d1471005172b1
SHA512	46a52631e3dd49b0ae10afbdf50a08d6d6575f3093b3921b2fa744704e2d317f8b10a6d48ad7f922a7843731782521773032a6cc04833b00bd85e404c168ffe4

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-profile-l1-1-0.dll

MD5	7a629293eeb0bca5f9bdee8ade477c54
SHA1	a25bf8bac4fbfd9216ea827e71344ba07b1d463b
SHA256	7809160932f44e59b021699f5bc68799eb7293ee1fa926d6fcca3c3445302e61
SHA512	1c58c547d1fe9b54ddf07e5407edaf3375c6425ca357aa81d09c76a001376c43487476a6f18c891065ab99680501b0f43a16a10ed8e0d5e87b9a9542098f45fe

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-file-l1-2-0.dll

MD5	cc228ff8d86b608e73026b1e9960b2f8
SHA1	cef0705aee1e8702589524879a49e859505d6fe0
SHA256	4cadbc0c39da7c6722206fdcebd670abe5b8d261e7b041dd94f9397a89d1990d
SHA512	17abd9e0ec20b7eb686e3c0f41b043d0742ab7f9501a423b2d2922d44af660379792d1cc6221effbd7e856575d5babf72657ae9127c87cc5cf678bd2ceb1228f

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-processthreads-l1-1-0.dll

MD5	c123f2c161884fbff4f00ef1e1391266
SHA1	7db3055da53916bea2b85b159491a0772fb620ce
SHA256	5ccb89e93d67bc3288d4e84649c5346e66e15e3d7cd65d989daf3f4cb584be9a
SHA512	dac5616320b9052254b5687959e67126c4a938e79173d8245675a9651674384c36cc856f996ef88ae621ec67afc66166266575 85d92bb5d14602a7cc9fc0f669

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-processenvironment-l1-1-0.dll

MD5	7fd4a71085783ccfe9c289c07bcf9b04
SHA1	bb6ffdb5c069dbba06998dc877d24f72dad6298d
SHA256	c4eca98c3c67b6395d5b005b00ac1eb0318b86b23aa71035a44c2b1602befba9
SHA512	a96c5b90b8384b239be111d90caa3b947651ad73382ab9e5dbe4a4b6ad30921876545331d37c8d5a8f669e39d71bf60983c4ba39c479e23015c2f7579c5e55cd

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-namedpipe-l1-1-0.dll

MD5	4a28ca64f44b91f43945ee3971e0996a
SHA1	45b3d8584c58e8d6ae507fdbd772feeb1886c8b0
SHA256	c05f1fffe3b5a2738ea54ce9485cca026fb9635f982626fba1e1dcc531897273
SHA512	862a0428f08d447cd1ee0431969e0fbcb182f4c46418c26d26fa33e586e686d9c093c1ca5781f544ce9276195ce973850719636e39e465f059607f455ecfdd93

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-memory-l1-1-0.dll

MD5	8d285430e8bda6d5c9b683579adcb180
SHA1	619dbbcff06c659e3fc48f03917a4dadbfc1c275
SHA256	0512a35316ec9180437f86696a84c5c06a7e4e82e050055a656e5bf9fca206f9
SHA512	38405dd85dd62f843abb55acea1b64d7d63bb601445bf1b32078cde5bbef4861dd99f26659281fe2aea86f58cfb1725d8c63d91fb539dcbf5d98cdbe783337fc

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-localization-l1-2-0.dll

MD5	5241df2e95e31e73ccfd6357ad309df0
SHA1	2644cc5e86dfad1ad2140181ab2ca79725f95411
SHA256	6ee44dd0d8510dc024c9f7c79b1b9fa88c987b26b6beb6653ddd11751c34e5dc
SHA512	52cccd1dd237e764e34996c0c5f7a759a7f0eff29b61befeaf96a16d80df2ba9ee2c3615f875153198a145d68f275aea6d02187e6eee5a129e3e2ab81aaceb16

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-libraryloader-l1-1-0.dll

MD5	5fbcb20d99e463259b4f15429010b9cd
SHA1	b16770f8bb53dc2bafcb309824d6fa7b57044d8a
SHA256	7f39ba298b41e4963047341288cab36b6a241835ee11ba4ad70f44dacd40906c
SHA512	7ba1ac34b3ecfbfb8252f5875be381d8ef823b50dfe0e070222175ee51191f5ee6d541eeedd1445ed603a23d200ce9ce15914c8ed3fafe7e7f3591f51f896c58

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-kernel32-legacy-l1-1-1.dll

MD5	0c1cc0a54d4b38885e1b250b40a34a84
SHA1	24400f712bbe1dd260ed407d1eb24c35dcb2ecac
SHA256	a9b13a1cd1b8c19b0c6b4afcd5bb0dd29c0e2288231ac9e6db8510094ce68ba6
SHA512	71674e7ed8650cac26b6f11a05bfc12bd7332588d21cf81d827c1d22df5730a13c1e6b3ba797573bb05b3138f8d46091402e63c059650c7e33208d50973dde39

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-interlocked-l1-1-0.dll

MD5	86023497fa48ca2c7705d3f90b76ebc5
SHA1	835215d7954e57d33d9b34d8850e8dc82f6d09e8
SHA256	53b25e753ca785bf8b695d89dde5818a318890211dc992a89146f16658f0b606
SHA512	8f8370f4c0b27779d18529164fa40cbfddafa81a4300d9273713b13428d0367d50583271ea388d43c1a96fed5893448cd14711d5312da9dfa09b9893df333186

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-heap-l1-1-0.dll

MD5	344a09b4be069f86356a89482c156647
SHA1	2506ffeb157cb531195dd04d11d07c16e4429530
SHA256	8f105771b236dbcb859de271f0a6822ce1cb79c36988dd42c9e3f6f55c5f7eb9
SHA512	4c1e616443576dc83200a4f98d122065926f23212b6647b601470806151ff15ea44996364674821afec492b29ba868f188a9d6119b1e1d378a268f1584ca5b29

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-handle-l1-1-0.dll

MD5	416aa8314222db6cbb3760856be13d46
SHA1	5f28fe2d565378c033ef8eea874bc38f4b205327
SHA256	39095f59c41d76ec81bb2723d646fde4c148e7cc3402f4980d2ade95cb9c84f9
SHA512	b16ed31dc3343caea47c771326810c040a082e0ab65d9ae69946498ceb6ae0dee0a570dbcd88090668a100b952c1ff88bade148811b913c90931aa0e657cd808

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-file-l2-1-0.dll

MD5	e368a236f5676a3da44e76870cd691c9
SHA1	e4f1d2c6f714a47f0dc29021855c632ef98b0a74
SHA256	93c624b366ba16c643fc8933070a26f03b073ad0cf7f80173266d67536c61989
SHA512	f5126498a8b65ab20afaaf6b0f179ab5286810384d44638c35f3779f37e288a51c28bed3c3f8125d51feb2a0909329f3b21273cb33b3c30728b87318480a9ef8

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-file-l1-1-0.dll

MD5	9f45a47ebfd9d0629f4935764243dd5a
SHA1	86a4a0ea205e31fb73f3bfcce24945bd6bea06c7
SHA256	1ca895aba4e7435563a6b43e85eba67a0f8c74aa6a6a94d0fc48fa35535e2585
SHA512	8c1cdcad557bff1685a633d181fcf14ec512d322caeaeb9c937da8794c74694fe93528fc9578cb75098f50a2489ed4a5dedf8c8c2ac93eeb9c8f50e3dd690d5f

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-fibers-l1-1-1.dll

MD5	050a30a687e7a2fa6f086a0db89aa131
SHA1	1484322caaf0d71cbb873a2b87bdd8d456da1a3b
SHA256	fc9d86cec621383eab636ebc87ddd3f5c19a3cb2a33d97be112c051d0b275429
SHA512	07a15aa3b0830f857b9b9ffeb57b6593ae40847a146c5041d38be9ce3410f58caa091a7d5671cc1bc7285b51d4547e3004cf0e634ae51fe3da0051e54d8759e1

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-fibers-l1-1-0.dll

MD5	b5e2760c5a46dbeb8ae18c75f335707e
SHA1	e71db44fc0e0c125de90a9a87ccb1461e72a9030
SHA256	91d249d7bc0e38ef6bcb17158b1fdc6dd8888dc086615c9b8b750b87e52a5fb3
SHA512	c3400772d501c5356f873d96b95dc33428a34b6fcaad83234b6782b5f4bf087121e4fd84885b1abab202066da98eb424f93dd2eed19a0e2a9f6ff4a5cfd1e4f3

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-errorhandling-l1-1-0.dll

MD5	c2f8c03ecce9941492bfbe4b82f7d2d5
SHA1	909c66c6dfea5e0c74d3892d980918251bb08632
SHA256	d56ce7b1cd76108ad6c137326ec694a14c99d48c3d7b0ace8c3ff4d9bcee3ce8
SHA512	7c6c85e390bbe903265574e0e7a074da2ce30d9376d7a91a121a3e0b1a8b0fffd5579f404d91836525d4400d2760cb74c9cb448f8c5ae9713385329612b074cf

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-debug-l1-1-0.dll

MD5	226a5983ae2cbbf0c1bda85d65948abc
SHA1	d0f131dcba0f0717c5dea4a9ca7f2e2ecf0ad1c3
SHA256	591358eb4d1531e9563ee0813e4301c552ce364c912ce684d16576eabf195dc3
SHA512	a1e6671091bd5b2f83bfaa8fcf47093026e354563f84559bd2b57d6e9fa1671eea27b4ed8493e9fdf4bde814074dc669de047b4272b2d14b4f928d25c4be819d

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-datetime-l1-1-0.dll

MD5	8f8eb9cb9e78e3a611bc8acaec4399cb
SHA1	237eee6e6e0705c4be7b0ef716b6a4136bf4e8a8
SHA256	1bd81dfd19204b44662510d9054852fb77c9f25c1088d647881c9b976cc16818
SHA512	5b10404cdc29e9fc612a0111b0b22f41d78e9a694631f48f186bdde940c477c88f202377e887b05d914108b9be531e6790f8f56e6f03273ab964209d83a60596

C:\Users\Admin\AppData\Local\Temp_MEI34722\api-ms-win-core-console-l1-1-0.dll

MD5	9f746f4f7d845f063fea3c37dcebc27c
SHA1	24d00523770127a5705fcc2a165731723df36312
SHA256	88ace577a9c51061cb7d1a36babbbefa48212fadc838ffde98fdfff60de18386
SHA512	306952418b095e5cf139372a7e684062d05b2209e41d74798a20d7819efeb41d9a53dc864cb62cc927a98df45f7365f32b72ec9b17ba1aee63e2bf4e1d61a6e4

memory/3416-1835-0x000001E519BA0000-0x000001E51AF1E000-memory.dmp

Part 5. Analysis: behavioral1

5. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-12-27 22:39	2025-12-27 22:48	win10v2004-20251223-en	150s	155s

5. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe"
```

5. 3. Signatures

A potential corporate email address has been identified in the URL:

phishing

Loads dropped DLL

Description	Indicator	Process	Target
N/A	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	N/A

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A

Browser Information Discovery

discovery

Enumerates physical storage devices

System Time Discovery

discovery

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

Checks processor information in registry

Description	Indicator	Process	Target
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\VendorIdentifier	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key opened	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key value queried	\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0\VendorIdentifier	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Enumerates system info in registry

Description	Indicator	Process	Target
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 (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 (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

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 = "134113492341042481"	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-19\Software\Microsoft\Cryptography\TPM\Telemetry	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Modifies registry class

Description	Indicator	Process	Target
Key created	\REGISTRY\USER\S-1-5-21-1404556474-4089494618-1653937001-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\Instance\	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{1f3427c8-5c10-4210-aa03-2ee45287d668}\Instance\	C:\Program Files (x86)\Microsoft\Edge\Application\ms	N/A

Description	Indicator	Process	Target
		edge.exe	
Key created	\REGISTRY\MACHINE\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-1404556474-4089494618-1653937001-1000\{43B6F772-64B6-474F-BC17-4DFB01402499}	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A
Key created	\REGISTRY\USER\S-1-5-21-1404556474-4089494618-1653937001-1000_Classes\CLSID\{018D5C66-4533-4307-9B53-224DE2ED1FE6}\Instance\	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.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
Key created	\REGISTRY\MACHINE\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\Deployment\Package*\S-1-5-21-1404556474-4089494618-1653937001-1000\{6E8F5CE9-6463-4BBF-80E7-BE477508E4DD}	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	N/A

Suspicious behavior: EnumeratesProcesses

Description	Indicator	Process	Target
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
N/A	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.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
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
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
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

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
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
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
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
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
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
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
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
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
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
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 AdjustPrivilegeToken

Description	Indicator	Process	Target
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	N/A
Token: SeDebugPrivilege	N/A	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.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
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 WriteProcessMemory

Description	Indicator	Process	Target
PID 4204 wrote to memory of 3076	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe
PID 3076 wrote to memory of 3224	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Description	Indicator	Process	Target
PID 3076 wrote to memory of 6028	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 3076 wrote to memory of 1432	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 3076 wrote to memory of 5240	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 3076 wrote to memory of 5328	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 3076 wrote to memory of 4368	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 3076 wrote to memory of 372	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 3076 wrote to memory of 4560	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 3076 wrote to memory of 3592	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 3076 wrote to memory of 4900	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PID 3076 wrote to memory of 5132	N/A	C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5348	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 1604	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 1040	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 1040	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 1040	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 816	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 816	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 2216	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5088	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 2216	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 2216	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5088	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5088	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4388	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4388	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4728	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4728	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5824	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe
PID 5132 wrote to memory of 5492	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5492	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5492	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5632	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5632	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 5132 wrote to memory of 5632	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5256	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5256	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5256	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5968	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5968	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5968	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 2392	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 2392	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 2392	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5004	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5004	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5004	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5216	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5216	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 5216	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4640	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4640	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4640	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4624	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4624	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4624	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4704	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4704	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4704	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4580	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4580	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4580	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
PID 5132 wrote to memory of 4452	N/A	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

5. 4. Processes

C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe

```
"C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe"
```

C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe

```
"C:\Users\Admin\AppData\Local\Temp\Radar_Inwestora_v4_3 (2).exe"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Google News]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

Google is at last letting users swap out embarrassing Gmail addresses without losing their data - Los Angeles Times

<ol><li><a
href=\"https://news.google.com/rss/articles/CBMitwFBVV95cUxNVk8wTDFMUkxiRUY2ZzhfUnBuLTdIWGY0ZlVaZ2ozODYybXZRNWlwMnVKQ1dzSE5UTjZ5bjBBdi11N2tZd
</text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Google News\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Google News]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

Google founder Sergey Brin tells Stanford engineering students: I made the mistake of thinking I am the n - Times of India

<a
href=\"https://news.google.com/rss/articles/CBMiuwJBVV95cUxNdFZRVzhxT1hRd2h1ZkNvdzJUdUhoTUdIT2dIendWTnpwclJUR3piaTI0cWN4RVotcktjdUxIWm5xQU1Me
</text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Google News\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Google News]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

The single best Google Keep feature that turned me into a power user - Android Police

<a
href=\"https://news.google.com/rss/articles/CBMiiwFBVV95cUxNMERmcExJQWtGTXVrQWhtMGlSTUs3RF9xSFZ5NWljS05GTWhQRUtidDZqSlgtYTlKU0lqV3RVcEo3Q0l3d
</text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Google News\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Google News]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

Google Phone adding ‘Keep portrait mode’ setting [U: Rolled back] - 9to5Google

<a
href=\"https://news.google.com/rss/articles/CBMickFVX3lxTE5zc2V5TW1Qcm9qR1NpQVpYZ1I4dFM4di0yY1kxRnVJTFBPMGZQUC1nTWlwd0owSnEwNHBibEF0YmdKNlNkN
</text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Google News\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Google News]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

Why Apple and Google want your ID - Fast Company

<a
href=\"https://news.google.com/rss/articles/CBMifkFVX3lxTE9RX0gwNkItSFRoOEg0bUo5aUtoLUQ1cEk3V0VKQW1NUnc4c0doanFrUFctTGN2WUR0cm1aZm5rVDJGaXcwC
</text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Google News\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Yahoo Finance]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

Nvidia Has Tumbled From All-Time Highs in October. Here's What's Next.

It's still beating the market by far for the year.]]></text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Yahoo Finance\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Yahoo Finance]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

Alphabet Crushed Mag 7 Stocks This Year — Only To Be Crushed By These 8 Country ETFs

Alphabet Inc. (NASDAQ:GOOG) (NASDAQ:GOOGL) is on pace to top the 2025 Magnificent Seven leaderboard, but investors who looked beyond U.S.
tech found even richer returns across eight different global e]]></text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Yahoo Finance\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Yahoo Finance]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

The Best Stocks to Invest $50,000 in Right Now

If you're investing for the long run, there are a myriad of companies begging to be bought.]]></text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Yahoo Finance\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Yahoo Finance]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

Billionaire Chase Coleman Has Formed His Own \"Magnificent Seven\" and It's Even Better Than the Original

The new \"Magnificent Seven\" is better suited for today's current market.]]></text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Yahoo Finance\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
powershell.exe -ExecutionPolicy Bypass -Command "
[Windows.UI.Notifications.ToastNotificationManager, Windows.UI.Notifications, ContentType = WindowsRuntime] > $null
[Windows.UI.Notifications.ToastNotification, Windows.UI.Notifications, ContentType = WindowsRuntime] | Out-Null
[Windows.Data.Xml.Dom.XmlDocument, Windows.Data.Xml.Dom.XmlDocument, ContentType = WindowsRuntime] | Out-Null
$Template = @\"
<toast  duration=\"long\">
    <visual>
        <binding template=\"ToastImageAndText02\">
            <image id=\"1\" src=\"\" />
            <text id=\"1\"><![CDATA[MEDIUM | Yahoo Finance]]></text>
            <text id=\"2\"><![CDATA[😐 NEUTRAL (+0.00)

Google's Gemini Eating ChatGPT's Lunch: Market Share Gain From 5% To 18% Is 'Clearest Signal' That Alphabet Is Winning AI War

Alphabet Inc.'s (NASDAQ:GOOG) (NASDAQ:GOOGL) Gemini is executing a silent takeover of the generative AI market, surging to an 18.2% traffic
share in just one year while industry pioneer ChatGPT suffer]]></text>
        </binding>
    </visual>
    <actions>

    </actions>
    <audio src=\"ms-winsoundevent:Notification.Default\" loop=\"false\" />
</toast>
\"@

$SerializedXml = New-Object Windows.Data.Xml.Dom.XmlDocument
$SerializedXml.LoadXml($Template)

$Toast = [Windows.UI.Notifications.ToastNotification]::new($SerializedXml)
$Toast.Tag = \"MEDIUM | Yahoo Finance\"
$Toast.Group = \"Investment Radar\"

$Notifier = [Windows.UI.Notifications.ToastNotificationManager]::CreateToastNotifier(\"Investment Radar\")
$Notifier.Show($Toast);
"
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument https://finance.yahoo.com/news/googles-gemini-eating-
chatgpts-lunch-163103026.html?.tsrc=rss
```

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=139.0.7258.155 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --
annotation=plat=Win64 --annotation=prod=Edge --annotation=ver=139.0.3405.125 --initial-client-
data=0x2c0,0x2c4,0x2c8,0x2bc,0x2d0,0x7ffb7c83c188,0x7ffb7c83c194,0x7ffb7c83c1a0
```

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 --no-pre-read-main-dll --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=1968,i,15112744601905925294,11237071724358370574,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=2344 /prefetch:3
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-pre-read-main-dll --force-high-res-timeticks=disabled --gpu-preferences=SAAAAAAAAADgAAAIAAAAAAAAAAAAAGAAAQAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --always-read-main-dll --metrics-shmem-handle=1760,i,16649682057573127726,10468674992713188242,262144 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=2304 /prefetch:2
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\elevation_service.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\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=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=2620,i,3486086902330848746,3741158845522183629,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=2768 /prefetch:8
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --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 --metrics-shmem-handle=3404,i,2294355544000151390,6097659391527848095,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=3480 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --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 --metrics-shmem-handle=3408,i,4374752939529011643,8667188935430765730,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=3484 /prefetch:1
```

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 --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4972,i,8779841257821662357,15293822549026747995,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=5024 /prefetch:8
```

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 --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4984,i,6052114612556380728,373196792477213712,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=5048 /prefetch:8
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5780,i,4013734961692222210,6572117590897443661,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=5792 /prefetch:8
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=5780,i,4013734961692222210,6572117590897443661,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=5792 /prefetch:8
```

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=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=10 --always-read-main-dll --metrics-shmem-handle=6208,i,15847090867433807325,1831611281934719620,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=6224 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=11 --always-read-main-dll --metrics-shmem-handle=6192,i,17472635226429893548,17253629644046292561,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=6264 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=12 --always-read-main-dll --metrics-shmem-handle=6460,i,14601869171457591299,10773746574869136374,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=6472 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=13 --always-read-main-dll --metrics-shmem-handle=6624,i,9931032304240981017,16160263761549979113,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=6616 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=14 --always-read-main-dll --metrics-shmem-handle=6804,i,170446657255516586,9335528804016717334,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=6808 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=15 --always-read-main-dll --metrics-shmem-handle=6912,i,1369460328614602136,11683888735425030170,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=6932 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=16 --always-read-main-dll --metrics-shmem-handle=6956,i,12126247894822065414,16503860741659641688,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7092 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=17 --always-read-main-dll --metrics-shmem-handle=7236,i,10150703820092596l3,7226804525215938676,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7136 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=18 --always-read-main-dll --metrics-shmem-handle=7284,i,11224349911826324934,5310036210358447217,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7384 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=19 --always-read-main-dll --metrics-shmem-handle=7524,i,13682785432685450421,15374447019013659836,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7528 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=20 --always-read-main-dll --metrics-shmem-handle=7680,i,14456032222665226805,10686300154171569173,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7696 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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 --metrics-shmem-handle=7832,i,5772110895050023363,7537942657971923,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7856 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=22 --always-read-main-dll --metrics-shmem-handle=7996,i,9897721399455753248,4971013391404040327,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7884 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=23 --always-read-main-dll --metrics-shmem-handle=8136,i,12419025691695008131,4920114268399147713,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=8144 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=24 --always-read-main-dll --metrics-shmem-handle=8296,i,12415035098098784556,13692532897391401304,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=8304 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=25 --always-read-main-dll --metrics-shmem-handle=8448,i,8562915780980484252,6583695669022352227,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=8456 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=26 --always-read-main-dll --metrics-shmem-handle=8600,i,5120684040614636973,13847352265350535788,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=8608 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=27 --always-read-main-dll --metrics-shmem-handle=8752,i,11568403498562248354,6517572781803928063,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=8768 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=28 --always-read-main-dll --metrics-shmem-handle=6904,i,16010616139680184767,1862246568467283110,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=9048 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=29 --always-read-main-dll --metrics-shmem-handle=9160,i,7887723154428787343,4995253860786134230,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=9300 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=30 --always-read-main-dll --metrics-shmem-handle=9444,i,8936061875949140097,3733946622924641307,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=9448 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=31 --always-read-main-dll --metrics-shmem-handle=7832,i,11413966329241868946,864729485797649954,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=8448 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=32 --always-read-main-dll --metrics-shmem-handle=9632,i,1725690494786748664,11929637242694129717,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=9272 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --lang=en-US --service-sandbox-type=audio --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=9800,i,10838402701516994775,7622705599497797077,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=9820 /prefetch:8
```

C:\Windows\system32\AUDIODG.EXE

```
C:\Windows\system32\AUDIODG.EXE 0x244 0x3c8
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=34 --always-read-main-dll --metrics-shmem-handle=9972,i,14379765809523813427,17599853165091735654,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10000 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=35 --always-read-main-dll --metrics-shmem-handle=10124,i,13370082027931437703,10005369827721571511,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10164 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=36 --always-read-main-dll --metrics-shmem-handle=10316,i,2384369853814324175,1487913384236474058,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10344 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=37 --always-read-main-dll --metrics-shmem-handle=10168,i,17001679650961802866,16845120667051912250,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10460 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=38 --always-read-main-dll --metrics-shmem-handle=10652,i,11308343034516721434,7360874463670136757,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10648 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=39 --always-read-main-dll --metrics-shmem-handle=10676,i,18159877990827653792,17818643227860346676,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10852 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=40 --always-read-main-dll --metrics-shmem-handle=10964,i,3203251656687038102,4407210741867167970,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10980 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=41 --always-read-main-dll --metrics-shmem-handle=11128,i,11293591700664372903,12849851386232924817,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=11184 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=42 --always-read-main-dll --metrics-shmem-handle=10676,i,12078690631576400413,9362903040251435206,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10120 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=43 --always-read-main-dll --metrics-shmem-handle=10800,i,5923141968592781204,1712293677316166603,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10664 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=44 --always-read-main-dll --metrics-shmem-handle=7264,i,11244397971245440171,14004037882135154204,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7532 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=45 --always-read-main-dll --metrics-shmem-handle=7876,i,12837981603422861685,4082478716170163022,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=8020 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=46 --always-read-main-dll --metrics-shmem-handle=10868,i,3829125981510612494,5514050632607936572,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10940 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=47 --always-read-main-dll --metrics-shmem-handle=10756,i,2171301872970754625,12396100152052086425,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7592 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=48 --always-read-main-dll --metrics-shmem-handle=8212,i,3908756488772050922,7985602707992686761,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=11280 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=49 --always-read-main-dll --metrics-shmem-handle=10900,i,15426161666096530439,15543270643633957153,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10716 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=50 --always-read-main-dll --metrics-shmem-handle=7976,i,2258351593600485393,12682468197048439150,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=8268 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=51 --always-read-main-dll --metrics-shmem-handle=10372,i,10940547035990300813,1969079358159000506,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10456 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --disable-gpu-compositing --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=52 --always-read-main-dll --metrics-shmem-handle=10384,i,1743862551646741986,17747486747849721662,2097152 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=10780 /prefetch:1
```

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 --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=8132,i,5908937914053724701,2526130596856460559,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7840 /prefetch:8
```

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 --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=10352,i,1524056391414930090,13536365790343884714,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=7596 /prefetch:8
```

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 --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=10760,i,6597229961362887876,3951693573237608659,524288 --field-trial-handle=2308,i,8823099187625646362,6400410809173822889,262144 --variations-seed-version --mojo-platform-channel-handle=11248 /prefetch:8
```

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

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

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=139.0.7258.155 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 --annotation=prod=Edge --annotation=ver=139.0.3405.125 --initial-client-data=0x238,0x23c,0x240,0x234,0x24c,0x7ffb7c83c188,0x7ffb7c83c194,0x7ffb7c83c1a0
```

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 --no-pre-read-main-dll --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=1928,i,8361855715042794805,2294278463651753128,524288 --field-trial-handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=2316 /prefetch:3
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --no-pre-read-main-dll --force-high-res-timeticks=disabled --gpu-preferences=SAAAAAAAAADgAAAIAAAAAAAAAAAAGAAAQAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAACAAAAAAAAAAIAAAAAAAAAA== --always-read-main-dll --metrics-shmem-handle=1744,i,14299168279229868472,11629709022524005079,262144 --field-trial-handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=2284 /prefetch:2
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\elevation_service.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\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=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=2596,i,14127465596995665914,12230310285099055023,524288 --field-trial-handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=2584 /prefetch:8
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4628,i,4068113674074322260,17489268888166532546,524288 --field-trial-handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=4644 /prefetch:8
```

C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe

```
"C:\Program Files (x86)\Microsoft\Edge\Application\139.0.3405.125\identity_helper.exe" --type=utility --utility-sub-type=winrt_app_id.mojom.WinrtAppIdService --lang=en-US --service-sandbox-type=none --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-handle=4628,i,4068113674074322260,17489268888166532546,524288 --field-trial-handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=4644 /prefetch:8
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument https://buymeacoffee.com/kitay
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --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=7 --always-read-main-dll --metrics-shmem-handle=5040,i,10204319428487554622,10219637280941713305,2097152 --field-trial-handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=5088 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --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 --metrics-shmem-handle=5052,i,2842075045356649088,12345728242182434254,2097152 --field-trial-handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=5096 /prefetch:1
```

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 --force-high-res-timeticks=disabled --always-read-main-dll --metrics-shmem-
handle=5576,i,7712037003984094088,16807171218761964802,524288 --field-trial-handle=2288,i,10294448964470514254,16801396959534837202,262144
--variations-seed-version --mojo-platform-channel-handle=5024 /prefetch:8
```

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 --force-high-res-timeticks=disabled --always-read-main-dll --
metrics-shmem-handle=5588,i,14950788945904426273,1296507616530966078,524288 --field-trial-
handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=5648 /prefetch:8
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --
disable-gpu-compositing --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=10 --always-read-main-dll --metrics-shmem-
handle=5604,i,17079443364066590815,14456546553283568104,2097152 --field-trial-
handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=6016 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --
disable-gpu-compositing --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=11 --always-read-main-dll --metrics-shmem-
handle=6204,i,14259702029725790093,12280465860115843995,2097152 --field-trial-
handle=2288,i,10294448964470514254,16801396959534837202,262144 --variations-seed-version --mojo-platform-channel-handle=6216 /prefetch:1
```

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

```
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --pdf-upsell-enabled --force-high-res-timeticks=disabled --
disable-gpu-compositing --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=12 --always-read-main-dll --metrics-shmem-
handle=6408,i,2953765531580699354,16070886846291900101,2097152 --field-trial-handle=2288,i,10294448964470514254,16801396959534837202,262144
--variations-seed-version --mojo-platform-channel-handle=6400 /prefetch:1
```

5. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	news.google.com	udp
NL	192.178.223.113:443	news.google.com	tcp
US	8.8.8.8:53	finance.yahoo.com	udp
GB	87.248.114.12:443	finance.yahoo.com	tcp
US	8.8.8.8:53	feeds.finance.yahoo.com	udp
IE	87.248.100.212:443	feeds.finance.yahoo.com	tcp
US	8.8.8.8:53	seekingalpha.com	udp
US	151.101.65.91:443	seekingalpha.com	tcp
US	8.8.8.8:53	c.pki.goog	udp
GB	142.251.29.94:80	c.pki.goog	tcp
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	finance.yahoo.com	udp
US	8.8.8.8:53	finance.yahoo.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	copilot.microsoft.com	udp
US	8.8.8.8:53	copilot.microsoft.com	udp
US	150.171.28.11:80	edge.microsoft.com	tcp
GB	87.248.114.11:443	finance.yahoo.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	104.18.22.222:443	copilot.microsoft.com	udp
US	104.18.22.222:443	copilot.microsoft.com	tcp
GB	87.248.114.11:443	finance.yahoo.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	guce.yahoo.com	udp
US	8.8.8.8:53	guce.yahoo.com	udp
IE	108.128.125.183:443	guce.yahoo.com	tcp
US	8.8.8.8:53	consent.yahoo.com	udp
US	8.8.8.8:53	consent.yahoo.com	udp
IE	34.250.129.70:443	consent.yahoo.com	tcp
US	8.8.8.8:53	s.yimg.com	udp
US	8.8.8.8:53	s.yimg.com	udp
IE	34.250.129.70:443	consent.yahoo.com	tcp

GB	87.248.114.12:443	s.yimg.com	tcp
GB	87.248.114.12:443	s.yimg.com	tcp
GB	87.248.114.12:443	s.yimg.com	tcp
GB	87.248.114.12:443	s.yimg.com	tcp
GB	87.248.114.12:443	s.yimg.com	tcp
US	8.8.8.8:53	udc.yahoo.com	udp
US	8.8.8.8:53	udc.yahoo.com	udp
IE	188.125.72.139:443	udc.yahoo.com	tcp
GB	92.123.128.175:443	www.bing.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.28.11:443	edge.microsoft.com	tcp
US	150.171.28.11:443	edge.microsoft.com	tcp
N/A	224.0.0.251:5353		udp
US	8.8.8.8:53	geo.yahoo.com	udp
US	8.8.8.8:53	geo.yahoo.com	udp
IE	188.125.72.139:443	geo.yahoo.com	tcp
GB	92.123.128.175:443	www.bing.com	udp
IE	34.250.129.70:443	consent.yahoo.com	tcp
IE	34.250.129.70:443	consent.yahoo.com	tcp
IE	108.128.125.183:443	consent.yahoo.com	tcp
GB	87.248.114.11:443	s.yimg.com	tcp
US	8.8.8.8:53	cdn.jsdelivr.net	udp
US	8.8.8.8:53	cdn.jsdelivr.net	udp
GB	87.248.114.12:443	s.yimg.com	tcp
US	8.8.8.8:53	query2.finance.yahoo.com	udp
US	8.8.8.8:53	query2.finance.yahoo.com	udp
GB	87.248.114.12:443	query2.finance.yahoo.com	tcp
GB	87.248.114.11:443	query2.finance.yahoo.com	tcp
US	151.101.193.229:443	cdn.jsdelivr.net	tcp
US	8.8.8.8:53	consent.cmp.oath.com	udp
US	8.8.8.8:53	consent.cmp.oath.com	udp
US	8.8.8.8:53	query1.finance.yahoo.com	udp
US	8.8.8.8:53	query1.finance.yahoo.com	udp
GB	87.248.114.11:443	query1.finance.yahoo.com	tcp
US	18.239.105.54:443	consent.cmp.oath.com	tcp
US	8.8.8.8:53	securepubads.g.doubleclick.net	udp
US	8.8.8.8:53	securepubads.g.doubleclick.net	udp
GB	142.251.29.155:443	securepubads.g.doubleclick.net	udp
GB	142.251.29.155:443	securepubads.g.doubleclick.net	tcp
US	18.239.105.54:443	consent.cmp.oath.com	tcp
US	8.8.8.8:53	opus.analytics.yahoo.com	udp
US	8.8.8.8:53	opus.analytics.yahoo.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.27.11:443	edge.microsoft.com	tcp
NL	18.238.243.123:443	opus.analytics.yahoo.com	tcp
US	8.8.8.8:53	wnsrvbjmeprtfrnfx.ay.delivery	udp
US	8.8.8.8:53	wnsrvbjmeprtfrnfx.ay.delivery	udp
US	104.21.41.177:443	wnsrvbjmeprtfrnfx.ay.delivery	tcp
US	8.8.8.8:53	i.clean.gg	udp
US	8.8.8.8:53	i.clean.gg	udp
US	8.8.8.8:53	sb.scorecardresearch.com	udp
US	8.8.8.8:53	sb.scorecardresearch.com	udp
US	34.95.69.49:443	i.clean.gg	tcp
NL	18.239.83.91:443	sb.scorecardresearch.com	tcp
US	34.95.69.49:443	i.clean.gg	udp
US	8.8.8.8:53	pbs.yahoo.com	udp
US	8.8.8.8:53	pbs.yahoo.com	udp
US	8.8.8.8:53	c2shb-oao.ssp.yahoo.com	udp
US	8.8.8.8:53	c2shb-oao.ssp.yahoo.com	udp
US	8.8.8.8:53	ads.yieldmo.com	udp
US	8.8.8.8:53	ads.yieldmo.com	udp
IE	18.202.183.91:443	c2shb-oao.ssp.yahoo.com	tcp
US	8.8.8.8:53	ups.analytics.yahoo.com	udp
US	8.8.8.8:53	ups.analytics.yahoo.com	udp

IE	3.255.12.221:443	ads.yieldmo.com	tcp
US	8.8.8.8:53	display.bidder.taboola.com	udp
US	8.8.8.8:53	display.bidder.taboola.com	udp
US	8.8.8.8:53	exchange.kueezrtb.com	udp
US	8.8.8.8:53	exchange.kueezrtb.com	udp
US	8.8.8.8:53	prebid.media.net	udp
US	8.8.8.8:53	prebid.media.net	udp
US	8.8.8.8:53	s.seedtag.com	udp
US	8.8.8.8:53	s.seedtag.com	udp
GB	87.248.114.11:443	ups.analytics.yahoo.com	tcp
US	151.101.1.44:443	display.bidder.taboola.com	tcp
US	34.36.209.34:443	prebid.media.net	tcp
US	137.184.241.143:443	exchange.kueezrtb.com	tcp
US	34.149.50.64:443	s.seedtag.com	tcp
IE	18.202.183.91:443	c2shb-oao.ssp.yahoo.com	tcp
US	8.8.8.8:53	sync.1rx.io	udp
US	8.8.8.8:53	sync.1rx.io	udp
US	34.238.229.121:443	sync.1rx.io	tcp
US	8.8.8.8:53	nexus-gateway-prod.media.yahoo.com	udp
US	8.8.8.8:53	nexus-gateway-prod.media.yahoo.com	udp
US	8.8.8.8:53	ads.pubmatic.com	udp
US	8.8.8.8:53	ads.pubmatic.com	udp
GB	2.22.44.196:443	ads.pubmatic.com	tcp
US	8.8.8.8:53	video-api.yql.yahoo.com	udp
US	8.8.8.8:53	video-api.yql.yahoo.com	udp
US	8.8.8.8:53	bats.video.yahoo.com	udp
US	8.8.8.8:53	bats.video.yahoo.com	udp
GB	87.248.114.11:443	bats.video.yahoo.com	tcp
US	8.8.8.8:53	hbx.media.net	udp
US	8.8.8.8:53	hbx.media.net	udp
GB	23.214.208.27:443	hbx.media.net	tcp
GB	23.214.208.27:443	hbx.media.net	tcp
US	8.8.8.8:53	api.taboola.com	udp
US	8.8.8.8:53	api.taboola.com	udp
US	151.101.193.44:443	api.taboola.com	tcp
US	34.36.209.34:443	prebid.media.net	udp
US	34.149.50.64:443	s.seedtag.com	udp
US	8.8.8.8:53	fb5f09bfc2fab43a93a528881a0b5c3c.safeframe.googlesyndication.com	udp
US	8.8.8.8:53	fb5f09bfc2fab43a93a528881a0b5c3c.safeframe.googlesyndication.com	udp
GB	142.250.129.132:443	fb5f09bfc2fab43a93a528881a0b5c3c.safeframe.googlesyndication.com	udp
GB	142.250.129.132:443	fb5f09bfc2fab43a93a528881a0b5c3c.safeframe.googlesyndication.com	udp
US	8.8.8.8:53	noa.yahoo.com	udp
US	8.8.8.8:53	noa.yahoo.com	udp
US	8.8.8.8:53	ib.adnxs.com	udp
US	8.8.8.8:53	ib.adnxs.com	udp
US	8.8.8.8:53	tsdtocl.com	udp
US	8.8.8.8:53	tsdtocl.com	udp
US	151.101.129.44:443	tsdtocl.com	tcp
NL	185.89.210.20:443	ib.adnxs.com	tcp
US	8.8.8.8:53	s.seedtag.com	udp
US	8.8.8.8:53	s.seedtag.com	udp
US	34.149.50.64:443	s.seedtag.com	tcp
US	151.101.129.44:443	tsdtocl.com	tcp
US	34.149.50.64:443	s.seedtag.com	tcp
US	151.101.193.229:443	cdn.jsdelivr.net	tcp
US	8.8.8.8:53	region1.google-analytics.com	udp
US	8.8.8.8:53	region1.google-analytics.com	udp
US	8.8.8.8:53	cs.seedtag.com	udp
US	8.8.8.8:53	cs.seedtag.com	udp
US	216.239.34.36:443	region1.google-analytics.com	tcp
US	8.8.8.8:53	pbs.yahoo.com	udp
US	8.8.8.8:53	pbs.yahoo.com	udp
US	104.16.56.62:443	cs.seedtag.com	udp
US	104.16.56.62:443	cs.seedtag.com	udp
GB	87.248.114.11:443	pbs.yahoo.com	tcp
US	8.8.8.8:53	u.openx.net	udp
US	8.8.8.8:53	u.openx.net	udp

US	35.244.159.8:443	u.openx.net	tcp
US	35.244.159.8:443	u.openx.net	tcp
US	8.8.8.8:53	secure-assets.rubiconproject.com	udp
US	8.8.8.8:53	secure-assets.rubiconproject.com	udp
US	8.8.8.8:53	csync.smartadserver.com	udp
US	8.8.8.8:53	csync.smartadserver.com	udp
US	8.8.8.8:53	ads.pubmatic.com	udp
US	8.8.8.8:53	ads.pubmatic.com	udp
US	8.8.8.8:53	ad.360yield.com	udp
US	8.8.8.8:53	ad.360yield.com	udp
US	8.8.8.8:53	visitor.omnitagjs.com	udp
US	8.8.8.8:53	visitor.omnitagjs.com	udp
US	8.8.8.8:53	onetag-sys.com	udp
US	8.8.8.8:53	onetag-sys.com	udp
US	8.8.8.8:53	match.sharethrough.com	udp
US	8.8.8.8:53	match.sharethrough.com	udp
US	8.8.8.8:53	csync.loopme.me	udp
US	8.8.8.8:53	csync.loopme.me	udp
US	8.8.8.8:53	match.prod.bidr.io	udp
US	8.8.8.8:53	match.prod.bidr.io	udp
US	8.8.8.8:53	sync.1rx.io	udp
US	8.8.8.8:53	sync.1rx.io	udp
US	8.8.8.8:53	sync.bfmio.com	udp
US	8.8.8.8:53	sync.bfmio.com	udp
US	8.8.8.8:53	cs.admanmedia.com	udp
US	8.8.8.8:53	cs.admanmedia.com	udp
US	8.8.8.8:53	streamer.finance.yahoo.com	udp
US	8.8.8.8:53	streamer.finance.yahoo.com	udp
US	35.244.159.8:443	u.openx.net	tcp
US	34.149.50.64:443	s.seedtag.com	udp
US	8.8.8.8:53	ib.adnxs.com	udp
US	8.8.8.8:53	ib.adnxs.com	udp
US	8.8.8.8:53	match.adsrvr.org	udp
US	8.8.8.8:53	match.adsrvr.org	udp
US	8.8.8.8:53	sync.smartadserver.com	udp
US	8.8.8.8:53	sync.smartadserver.com	udp
US	8.8.8.8:53	b1sync.zemanta.com	udp
US	8.8.8.8:53	b1sync.zemanta.com	udp
US	8.8.8.8:53	x.bidswitch.net	udp
US	8.8.8.8:53	x.bidswitch.net	udp
US	8.8.8.8:53	c1.adform.net	udp
US	8.8.8.8:53	c1.adform.net	udp
US	8.8.8.8:53	ap.lijit.com	udp
US	8.8.8.8:53	ap.lijit.com	udp
US	8.8.8.8:53	creativecdn.com	udp
US	8.8.8.8:53	creativecdn.com	udp
US	8.8.8.8:53	t.adx.opera.com	udp
US	8.8.8.8:53	t.adx.opera.com	udp
US	8.8.8.8:53	pong.chartbeat.net	udp
US	8.8.8.8:53	pong.chartbeat.net	udp
US	8.8.8.8:53	s.yimg.com	udp
US	8.8.8.8:53	s.yimg.com	udp
US	8.8.8.8:53	b.trueanthem.com	udp
US	8.8.8.8:53	b.trueanthem.com	udp
NL	35.214.236.30:443	csync.loopme.me	tcp
NL	35.214.236.30:443	csync.loopme.me	tcp
DE	18.153.64.118:443	match.sharethrough.com	tcp
DE	18.153.64.118:443	match.sharethrough.com	tcp
FR	34.1.1.166:443	visitor.omnitagjs.com	tcp
FR	34.1.1.166:443	visitor.omnitagjs.com	tcp
DE	51.38.120.206:443	onetag-sys.com	tcp
DE	51.38.120.206:443	onetag-sys.com	tcp
GB	2.22.44.196:443	ads.pubmatic.com	tcp
US	44.214.112.218:443	streamer.finance.yahoo.com	tcp
GB	2.22.44.196:443	ads.pubmatic.com	tcp
GB	2.19.117.77:443	csync.smartadserver.com	tcp
GB	23.215.239.190:443	secure-assets.rubiconproject.com	tcp

US	8.2.109.251:443	cs.admanmedia.com	tcp
US	35.212.17.176:443	sync.bfmio.com	tcp
IE	63.34.90.244:443	match.prod.bidr.io	tcp
IE	99.81.205.205:443	ad.360yield.com	tcp
US	52.7.91.107:443	sync.1rx.io	tcp
US	172.67.72.135:443	b.trueanthem.com	udp
GB	2.19.117.77:443	csync.smartadserver.com	tcp
GB	23.215.239.190:443	secure-assets.rubiconproject.com	tcp
US	8.2.109.251:443	cs.admanmedia.com	tcp
US	35.212.17.176:443	sync.bfmio.com	tcp
IE	63.34.90.244:443	match.prod.bidr.io	tcp
IE	99.81.205.205:443	ad.360yield.com	tcp
US	52.7.91.107:443	sync.1rx.io	tcp
NL	81.17.55.173:443	sync.smartadserver.com	tcp
NL	82.145.213.8:443	t.adx.opera.com	tcp
NL	185.184.8.90:443	creativecdn.com	tcp
IE	18.203.205.205:443	ap.lijit.com	tcp
US	35.71.131.137:443	match.adsrvr.org	tcp
US	35.71.131.137:443	match.adsrvr.org	tcp
NL	185.89.210.212:443	ib.adnxs.com	tcp
NL	35.214.136.108:443	x.bidswitch.net	tcp
GB	87.248.114.12:443	s.yimg.com	tcp
US	50.31.142.95:443	b1sync.zemanta.com	tcp
DK	37.157.6.230:443	c1.adform.net	tcp
SE	16.16.237.78:443	pong.chartbeat.net	tcp
US	8.8.8.8:53	cdn.ampproject.org	udp
US	8.8.8.8:53	cdn.ampproject.org	udp
US	8.8.8.8:53	tpc.googlesyndication.com	udp
US	8.8.8.8:53	tpc.googlesyndication.com	udp
US	8.8.8.8:53	securepubads.g.doubleclick.net	udp
US	8.8.8.8:53	securepubads.g.doubleclick.net	udp
US	8.8.8.8:53	image6.pubmatic.com	udp
US	8.8.8.8:53	image6.pubmatic.com	udp
US	8.8.8.8:53	trc.taboola.com	udp
US	8.8.8.8:53	trc.taboola.com	udp
NL	35.214.236.30:443	csync.loopme.me	tcp
DE	18.153.64.118:443	match.sharethrough.com	tcp
FR	34.1.1.166:443	visitor.omnitagjs.com	tcp
DE	51.38.120.206:443	onetag-sys.com	tcp
GB	2.22.44.196:443	ads.pubmatic.com	tcp
GB	2.19.117.77:443	csync.smartadserver.com	tcp
GB	23.215.239.190:443	secure-assets.rubiconproject.com	tcp
US	8.2.109.251:443	cs.admanmedia.com	tcp
US	35.212.17.176:443	sync.bfmio.com	tcp
IE	63.34.90.244:443	match.prod.bidr.io	tcp
IE	99.81.205.205:443	ad.360yield.com	tcp
US	52.7.91.107:443	sync.1rx.io	tcp
NL	81.17.55.173:443	sync.smartadserver.com	tcp
NL	82.145.213.8:443	t.adx.opera.com	tcp
NL	185.184.8.90:443	creativecdn.com	tcp
IE	18.203.205.205:443	ap.lijit.com	tcp
US	35.71.131.137:443	match.adsrvr.org	tcp
NL	185.89.210.212:443	ib.adnxs.com	tcp
NL	35.214.136.108:443	x.bidswitch.net	tcp
US	50.31.142.95:443	b1sync.zemanta.com	tcp
DK	37.157.6.230:443	c1.adform.net	tcp
SE	16.16.237.78:443	pong.chartbeat.net	tcp
US	172.67.72.135:443	b.trueanthem.com	tcp
NL	198.47.127.19:443	image6.pubmatic.com	tcp
GB	142.250.151.132:443	cdn.ampproject.org	tcp
GB	142.250.151.132:443	cdn.ampproject.org	tcp
GB	142.250.151.132:443	cdn.ampproject.org	tcp
GB	142.250.151.132:443	cdn.ampproject.org	tcp
GB	142.250.151.132:443	cdn.ampproject.org	tcp
GB	142.251.29.154:443	securepubads.g.doubleclick.net	udp
GB	142.250.140.132:443	tpc.googlesyndication.com	tcp
GB	142.250.140.132:443	tpc.googlesyndication.com	tcp

GB	142.251.29.155:443	securepubads.g.doubleclick.net	tcp
US	8.8.8.8:53	cdn.taboola.com	udp
US	8.8.8.8:53	cdn.taboola.com	udp
US	8.8.8.8:53	sync.kueezrtb.com	udp
US	8.8.8.8:53	sync.kueezrtb.com	udp
US	8.8.8.8:53	ads.yieldmo.com	udp
US	8.8.8.8:53	ads.yieldmo.com	udp
GB	23.214.208.27:443	hbx.media.net	udp
US	8.8.8.8:53	aax-eu.amazon-adsystem.com	udp
US	8.8.8.8:53	aax-eu.amazon-adsystem.com	udp
US	151.101.65.44:443	cdn.taboola.com	tcp
US	68.183.21.163:443	sync.kueezrtb.com	tcp
US	8.8.8.8:53	s.amazon-adsystem.com	udp
US	8.8.8.8:53	s.amazon-adsystem.com	udp
GB	23.214.208.27:443	hbx.media.net	udp
US	151.101.65.44:443	cdn.taboola.com	tcp
IE	54.170.123.81:443	ads.yieldmo.com	tcp
US	68.183.21.163:443	sync.kueezrtb.com	tcp
GB	142.250.140.132:443	tpc.googlesyndication.com	udp
US	8.8.8.8:53	eus.rubiconproject.com	udp
US	8.8.8.8:53	eus.rubiconproject.com	udp
IE	54.170.123.81:443	ads.yieldmo.com	tcp
IE	52.94.223.37:443	aax-eu.amazon-adsystem.com	tcp
US	98.82.156.207:443	s.amazon-adsystem.com	tcp
GB	23.37.197.145:443	eus.rubiconproject.com	tcp
GB	142.250.140.132:443	tpc.googlesyndication.com	udp
GB	142.250.140.132:443	tpc.googlesyndication.com	udp
US	8.8.8.8:53	players.brightcove.net	udp
US	8.8.8.8:53	players.brightcove.net	udp
US	151.101.194.27:443	players.brightcove.net	tcp
US	151.101.194.27:443	players.brightcove.net	tcp
US	151.101.194.27:443	players.brightcove.net	tcp
US	151.101.194.27:443	players.brightcove.net	tcp
US	151.101.194.27:443	players.brightcove.net	tcp
GB	142.251.29.154:443	securepubads.g.doubleclick.net	udp
US	8.8.8.8:53	www.google.com	udp
US	8.8.8.8:53	www.google.com	udp
US	8.8.8.8:53	metrics.brightcove.com	udp
US	8.8.8.8:53	metrics.brightcove.com	udp
US	8.8.8.8:53	static.chartbeat.com	udp
US	8.8.8.8:53	static.chartbeat.com	udp
GB	142.250.129.104:443	www.google.com	udp
US	35.244.232.184:443	metrics.brightcove.com	tcp
US	35.244.232.184:443	metrics.brightcove.com	tcp
FR	3.175.2.2:443	static.chartbeat.com	tcp
GB	142.250.129.104:443	www.google.com	tcp
US	8.8.8.8:53	match.sharethrough.com	udp
US	8.8.8.8:53	match.sharethrough.com	udp
DE	3.79.60.157:443	match.sharethrough.com	tcp
US	8.8.8.8:53	googleads.g.doubleclick.net	udp
US	8.8.8.8:53	googleads.g.doubleclick.net	udp
GB	142.250.151.155:443	googleads.g.doubleclick.net	udp
US	8.8.8.8:53	imasdk.googleapis.com	udp
US	8.8.8.8:53	imasdk.googleapis.com	udp
US	8.8.8.8:53	edge.api.brightcove.com	udp
US	8.8.8.8:53	edge.api.brightcove.com	udp
GB	142.250.117.95:443	imasdk.googleapis.com	tcp
US	151.101.194.27:443	edge.api.brightcove.com	tcp
US	8.8.8.8:53	rtb.gumgum.com	udp
US	8.8.8.8:53	rtb.gumgum.com	udp
IE	52.211.164.45:443	rtb.gumgum.com	tcp
IE	52.211.164.45:443	rtb.gumgum.com	tcp
US	35.244.232.184:443	metrics.brightcove.com	udp
US	8.8.8.8:53	manifest.prod.boltdns.net	udp
US	8.8.8.8:53	manifest.prod.boltdns.net	udp
GB	142.251.29.154:443	securepubads.g.doubleclick.net	udp
GB	142.250.117.95:443	imasdk.googleapis.com	udp

US	8.8.8.8:53	s0.2mdn.net	udp
US	8.8.8.8:53	s0.2mdn.net	udp
GB	142.250.117.148:443	s0.2mdn.net	tcp
US	8.8.8.8:53	tb.pbs.yahoo.com	udp
US	8.8.8.8:53	tb.pbs.yahoo.com	udp
GB	87.248.114.12:443	tb.pbs.yahoo.com	tcp
US	8.8.8.8:53	fastly-signed-us-east-1-prod.brightcovecdn.com	udp
US	8.8.8.8:53	fastly-signed-us-east-1-prod.brightcovecdn.com	udp
US	199.232.194.27:443	fastly-signed-us-east-1-prod.brightcovecdn.com	tcp
US	8.8.8.8:53	ping.chartbeat.net	udp
US	8.8.8.8:53	ping.chartbeat.net	udp
US	100.30.253.164:443	ping.chartbeat.net	tcp
NL	35.214.136.108:443	x.bidswitch.net	udp
US	8.8.8.8:53	www.temu.com	udp
US	8.8.8.8:53	www.temu.com	udp
US	8.8.8.8:53	b1sync.outbrain.com	udp
US	8.8.8.8:53	b1sync.outbrain.com	udp
US	50.31.142.95:443	b1sync.outbrain.com	tcp
US	172.66.1.242:443	www.temu.com	tcp
DK	37.157.6.230:443	c1.adform.net	tcp
US	8.8.8.8:53	cm.g.doubleclick.net	udp
US	8.8.8.8:53	cm.g.doubleclick.net	udp
US	172.217.76.155:443	cm.g.doubleclick.net	tcp
US	172.217.76.155:443	cm.g.doubleclick.net	tcp
US	35.71.131.137:443	match.adsrvr.org	tcp
US	8.8.8.8:53	tg.socdm.com	udp
US	8.8.8.8:53	tg.socdm.com	udp
US	172.217.76.155:443	cm.g.doubleclick.net	udp
JP	124.146.153.154:443	tg.socdm.com	tcp
JP	124.146.153.154:443	tg.socdm.com	tcp
NL	185.184.8.90:443	creativecdn.com	tcp
JP	124.146.153.154:443	tg.socdm.com	tcp
US	8.8.8.8:53	cs-server-s2s.yellowblue.io	udp
US	8.8.8.8:53	cs-server-s2s.yellowblue.io	udp
GB	23.37.197.145:443	eus.rubiconproject.com	tcp
US	8.8.8.8:53	token.rubiconproject.com	udp
US	8.8.8.8:53	token.rubiconproject.com	udp
US	34.4.35.11:443	cs-server-s2s.yellowblue.io	tcp
US	34.4.35.11:443	cs-server-s2s.yellowblue.io	tcp
US	8.8.8.8:53	ssc-cms.33across.com	udp
US	8.8.8.8:53	ssc-cms.33across.com	udp
NL	69.173.156.148:443	token.rubiconproject.com	tcp
US	67.202.105.24:443	ssc-cms.33across.com	tcp
US	67.202.105.24:443	ssc-cms.33across.com	tcp
DE	51.38.120.206:443	onetag-sys.com	udp
DE	51.38.120.206:443	onetag-sys.com	udp
US	67.202.105.24:443	ssc-cms.33across.com	tcp
US	8.8.8.8:53	ssbsync.smartadserver.com	udp
US	8.8.8.8:53	ssbsync.smartadserver.com	udp
US	8.8.8.8:53	ced-ns.sascdn.com	udp
US	8.8.8.8:53	ced-ns.sascdn.com	udp
US	8.8.8.8:53	trc.taboola.com	udp
US	8.8.8.8:53	trc.taboola.com	udp
NL	81.17.55.171:443	ssbsync.smartadserver.com	tcp
NL	81.17.55.171:443	ssbsync.smartadserver.com	tcp
GB	2.19.117.78:443	ced-ns.sascdn.com	tcp
US	8.8.8.8:53	bh.contextweb.com	udp
US	8.8.8.8:53	bh.contextweb.com	udp
US	8.8.8.8:53	ps.eyeota.net	udp
US	8.8.8.8:53	ps.eyeota.net	udp
DE	18.184.216.10:443	ps.eyeota.net	tcp
NL	208.93.169.131:443	bh.contextweb.com	tcp
US	8.8.8.8:53	ups.analytics.yahoo.com	udp
US	8.8.8.8:53	ups.analytics.yahoo.com	udp
US	8.8.8.8:53	secure.adnxs.com	udp
US	8.8.8.8:53	secure.adnxs.com	udp
US	8.8.8.8:53	us-u.openx.net	udp

US	8.8.8.8:53	us-u.openx.net	udp
US	8.8.8.8:53	sync.srv.stackadapt.com	udp
US	8.8.8.8:53	sync.srv.stackadapt.com	udp
US	8.8.8.8:53	sync.ipredictive.com	udp
US	8.8.8.8:53	sync.ipredictive.com	udp
US	8.8.8.8:53	match.deepintent.com	udp
US	8.8.8.8:53	match.deepintent.com	udp
NL	208.93.169.131:443	bh.contextweb.com	tcp
GB	87.248.114.12:443	ups.analytics.yahoo.com	tcp
US	3.222.175.162:443	sync.srv.stackadapt.com	tcp
US	34.203.78.19:443	sync.ipredictive.com	tcp
US	8.18.47.7:443	match.deepintent.com	tcp
US	8.8.8.8:53	usersync.gumgum.com	udp
US	8.8.8.8:53	usersync.gumgum.com	udp
IE	54.76.40.138:443	usersync.gumgum.com	tcp
DE	18.153.64.118:443	match.sharethrough.com	tcp
US	3.222.175.162:443	sync.srv.stackadapt.com	tcp
US	52.7.91.107:443	sync.1rx.io	tcp
US	8.8.8.8:53	ad.turn.com	udp
US	8.8.8.8:53	ad.turn.com	udp
NL	46.228.164.11:443	ad.turn.com	tcp
US	8.8.8.8:53	sync.richaudience.com	udp
US	8.8.8.8:53	sync.richaudience.com	udp
US	8.8.8.8:53	image8.pubmatic.com	udp
US	8.8.8.8:53	image8.pubmatic.com	udp
NL	35.214.236.30:443	csync.loopme.me	tcp
US	8.8.8.8:53	eb2.3lift.com	udp
US	8.8.8.8:53	eb2.3lift.com	udp
US	8.8.8.8:53	hb.trustedstack.com	udp
US	8.8.8.8:53	hb.trustedstack.com	udp
US	8.8.8.8:53	sync-service.net	udp
DE	148.251.40.153:443	sync.richaudience.com	tcp
US	35.244.159.8:443	us-u.openx.net	udp
US	8.8.8.8:53	jadserve.postrelease.com	udp
US	8.8.8.8:53	jadserve.postrelease.com	udp
US	8.8.8.8:53	ssum-sec.casalemedia.com	udp
US	8.8.8.8:53	ssum-sec.casalemedia.com	udp
NL	198.47.127.18:443	image8.pubmatic.com	tcp
NL	198.47.127.18:443	image8.pubmatic.com	tcp
US	13.248.245.213:443	eb2.3lift.com	tcp
US	204.62.12.209:443	sync-service.net	tcp
US	136.110.189.215:443	hb.trustedstack.com	tcp
US	104.18.27.193:443	ssum-sec.casalemedia.com	tcp
IE	52.211.245.241:443	jadserve.postrelease.com	tcp
US	8.8.8.8:53	id.rlcdn.com	udp
US	8.8.8.8:53	id.rlcdn.com	udp
US	8.8.8.8:53	csync.copper6.com	udp
US	8.8.8.8:53	csync.copper6.com	udp
US	35.244.174.68:443	id.rlcdn.com	tcp
US	80.77.84.97:443	csync.copper6.com	tcp
IE	54.76.40.138:443	usersync.gumgum.com	tcp
IE	54.76.40.138:443	usersync.gumgum.com	tcp
IE	54.76.40.138:443	usersync.gumgum.com	tcp
US	80.77.84.97:443	csync.copper6.com	tcp
US	8.8.8.8:53	rtb-csync.smartadserver.com	udp
US	8.8.8.8:53	rtb-csync.smartadserver.com	udp
FR	149.202.238.104:443	rtb-csync.smartadserver.com	tcp
US	104.18.27.193:443	ssum-sec.casalemedia.com	udp
US	8.8.8.8:53	cs.openwebmp.com	udp
US	8.8.8.8:53	cs.openwebmp.com	udp
US	50.31.142.95:443	b1sync.outbrain.com	tcp
DE	35.207.140.152:443	cs.openwebmp.com	tcp
US	80.77.84.97:443	csync.copper6.com	tcp
US	8.8.8.8:53	image6.pubmatic.com	udp
US	8.8.8.8:53	image6.pubmatic.com	udp
US	8.8.8.8:53	eu-u.openx.net	udp
US	8.8.8.8:53	eu-u.openx.net	udp

NL	46.228.164.11:443	ad.turn.com	tcp
US	104.18.27.193:443	ssum-sec.casalemedia.com	udp
DE	103.231.98.107:443	image6.pubmatic.com	tcp
US	34.98.64.218:443	eu-u.openx.net	tcp
DE	103.231.98.107:443	image6.pubmatic.com	tcp
US	8.8.8.8:53	dsp.nrich.ai	udp
US	8.8.8.8:53	dsp.nrich.ai	udp
FR	51.255.68.171:443	dsp.nrich.ai	tcp
US	8.8.8.8:53	visitor.europe-west9.gcp.omnitagjs.com	udp
US	8.8.8.8:53	visitor.europe-west9.gcp.omnitagjs.com	udp
FR	34.1.1.166:443	visitor.europe-west9.gcp.omnitagjs.com	tcp
US	8.8.8.8:53	pixel.rubiconproject.com	udp
US	8.8.8.8:53	pixel.rubiconproject.com	udp
NL	69.173.156.148:443	pixel.rubiconproject.com	tcp
NL	69.173.156.148:443	pixel.rubiconproject.com	tcp
US	8.8.8.8:53	csi.gstatic.com	udp
US	8.8.8.8:53	csi.gstatic.com	udp
US	172.217.12.131:443	csi.gstatic.com	tcp
US	8.8.8.8:53	pubads.g.doubleclick.net	udp
US	8.8.8.8:53	pubads.g.doubleclick.net	udp
GB	142.250.151.157:443	pubads.g.doubleclick.net	tcp
IE	18.203.205.205:443	ap.lijit.com	tcp
US	8.8.8.8:53	ce.lijit.com	udp
US	8.8.8.8:53	ce.lijit.com	udp
US	80.77.84.97:443	csync.copper6.com	tcp
IE	34.251.51.16:443	ce.lijit.com	tcp
US	8.8.8.8:53	sync.adotmob.com	udp
US	8.8.8.8:53	dsp-cookie.adfarm1.adition.com	udp
US	8.8.8.8:53	dsp-cookie.adfarm1.adition.com	udp
US	8.8.8.8:53	cms.quantserve.com	udp
US	8.8.8.8:53	cms.quantserve.com	udp
US	8.8.8.8:53	dis.criteo.com	udp
US	8.8.8.8:53	sync-tm.everesttech.net	udp
US	8.8.8.8:53	sync-tm.everesttech.net	udp
US	8.8.8.8:53	id5-sync.com	udp
US	8.8.8.8:53	id5-sync.com	udp
FR	45.137.176.88:443	sync.adotmob.com	tcp
DE	80.82.210.217:443	dsp-cookie.adfarm1.adition.com	tcp
US	151.101.194.49:443	sync-tm.everesttech.net	tcp
NL	35.214.236.30:443	csync.loopme.me	tcp
NL	178.250.1.129:443	dis.criteo.com	tcp
DE	91.228.74.244:443	cms.quantserve.com	tcp
DE	162.19.138.82:443	id5-sync.com	tcp
US	8.8.8.8:53	s.company-target.com	udp
US	8.8.8.8:53	s.company-target.com	udp
US	98.82.156.207:443	s.amazon-adsystem.com	tcp
US	34.96.71.22:443	s.company-target.com	tcp
US	8.8.8.8:53	wt.rqtrk.eu	udp
US	8.8.8.8:53	wt.rqtrk.eu	udp
US	98.82.156.207:443	s.amazon-adsystem.com	tcp
DE	57.129.18.105:443	wt.rqtrk.eu	tcp
US	8.8.8.8:53	equativ-match.dotomi.com	udp
US	8.8.8.8:53	equativ-match.dotomi.com	udp
NL	64.158.223.140:443	equativ-match.dotomi.com	tcp
US	172.66.1.242:443	www.temu.com	udp
US	98.82.156.207:443	s.amazon-adsystem.com	tcp
US	8.8.8.8:53	pbc.yahoo.com	udp
US	8.8.8.8:53	pbc.yahoo.com	udp
US	8.8.8.8:53	sync.visx.net	udp
US	8.8.8.8:53	i.ctnsnet.com	udp
US	8.8.8.8:53	i.ctnsnet.com	udp
DE	35.234.113.56:443	sync.visx.net	tcp
US	35.186.193.173:443	i.ctnsnet.com	tcp
US	8.8.8.8:53	bid.g.doubleclick.net	udp
US	8.8.8.8:53	bid.g.doubleclick.net	udp
US	172.217.76.155:443	bid.g.doubleclick.net	udp
US	172.217.12.131:443	csi.gstatic.com	udp

US	8.8.8.8:53	vast.doubleverify.com	udp
US	8.8.8.8:53	vast.doubleverify.com	udp
US	104.18.36.54:443	vast.doubleverify.com	udp
US	8.8.8.8:53	sync.kueezrtb.com	udp
US	8.8.8.8:53	sync.kueezrtb.com	udp
US	64.227.16.250:443	sync.kueezrtb.com	tcp
US	104.18.36.54:443	vast.doubleverify.com	tcp
US	8.8.8.8:53	secure.adnxs.com	udp
US	8.8.8.8:53	secure.adnxs.com	udp
DE	37.252.171.21:443	secure.adnxs.com	tcp
US	8.8.8.8:53	vpaid.doubleverify.com	udp
US	8.8.8.8:53	vpaid.doubleverify.com	udp
US	8.8.8.8:53	cdn.doubleverify.com	udp
US	8.8.8.8:53	cdn.doubleverify.com	udp
GB	142.250.117.148:443	s0.2mdn.net	udp
US	8.8.8.8:53	tps.doubleverify.com	udp
US	8.8.8.8:53	tps.doubleverify.com	udp
GB	2.16.153.5:443	cdn.doubleverify.com	tcp
US	8.8.8.8:53	rtb0.doubleverify.com	udp
US	8.8.8.8:53	rtb0.doubleverify.com	udp
US	172.64.155.111:443	vpaid.doubleverify.com	udp
US	8.8.8.8:53	vtrk.dv.tech	udp
US	8.8.8.8:53	vtrk.dv.tech	udp
US	130.211.44.5:443	rtb0.doubleverify.com	tcp
US	8.8.8.8:53	tpsc-video-eu.doubleverify.com	udp
US	8.8.8.8:53	tpsc-video-eu.doubleverify.com	udp
US	130.211.44.5:443	tpsc-video-eu.doubleverify.com	tcp
US	104.18.38.77:443	vtrk.dv.tech	udp
US	130.211.44.5:443	tpsc-video-eu.doubleverify.com	tcp
US	8.8.8.8:53	www.googletagservices.com	udp
US	8.8.8.8:53	www.googletagservices.com	udp
GB	142.250.151.157:443	pubads.g.doubleclick.net	udp
GB	142.250.140.155:443	www.googletagservices.com	tcp
US	8.8.8.8:53	ssp-sync.criteo.com	udp
US	8.8.8.8:53	ssp-sync.criteo.com	udp
US	8.8.8.8:53	gcdn.2mdn.net	udp
US	8.8.8.8:53	gcdn.2mdn.net	udp
NL	178.250.1.57:443	ssp-sync.criteo.com	tcp
NL	178.250.1.57:443	ssp-sync.criteo.com	tcp
NL	192.178.223.100:443	gcdn.2mdn.net	tcp
NL	192.178.223.100:443	gcdn.2mdn.net	tcp
US	8.8.8.8:53	r4---sn-aigl6nz7.c.2mdn.net	udp
US	8.8.8.8:53	r4---sn-aigl6nz7.c.2mdn.net	udp
GB	74.125.168.105:443	r4---sn-aigl6nz7.c.2mdn.net	udp
US	8.8.8.8:53	rtbc-ew1.doubleverify.com	udp
US	8.8.8.8:53	rtbc-ew1.doubleverify.com	udp
US	130.211.44.5:443	rtbc-ew1.doubleverify.com	tcp
US	130.211.44.5:443	rtbc-ew1.doubleverify.com	tcp
US	130.211.44.5:443	rtbc-ew1.doubleverify.com	tcp
US	130.211.44.5:443	rtbc-ew1.doubleverify.com	tcp
US	130.211.44.5:443	rtbc-ew1.doubleverify.com	tcp
NL	192.178.223.100:443	gcdn.2mdn.net	udp
US	8.8.8.8:53	bats.video.yahoo.com	udp
US	8.8.8.8:53	bats.video.yahoo.com	udp
US	8.8.8.8:53	pbd.yahoo.com	udp
US	8.8.8.8:53	pbd.yahoo.com	udp
US	8.8.8.8:53	a5203.casalemedia.com	udp
US	8.8.8.8:53	a5203.casalemedia.com	udp
US	130.211.44.5:443	rtbc-ew1.doubleverify.com	tcp
US	8.8.8.8:53	ade.googlesyndication.com	udp
US	8.8.8.8:53	ade.googlesyndication.com	udp
GB	142.250.117.148:443	s0.2mdn.net	udp
US	104.18.38.77:443	vtrk.dv.tech	udp
CA	85.91.45.117:443	a5203.casalemedia.com	tcp
GB	142.251.30.155:443	ade.googlesyndication.com	tcp
US	8.8.8.8:53	match.adsrvr.org	udp
US	8.8.8.8:53	match.adsrvr.org	udp

US	52.223.40.198:443	match.adsrvr.org	tcp
DE	3.79.60.157:443	match.sharethrough.com	tcp
GB	142.251.30.155:443	ade.googlesyndication.com	udp
US	8.8.8.8:53	sync.cootlogix.com	udp
US	8.8.8.8:53	sync.cootlogix.com	udp
US	157.245.95.194:443	sync.cootlogix.com	tcp
US	157.245.95.194:443	sync.cootlogix.com	tcp
GB	23.215.239.190:443	secure-assets.rubiconproject.com	tcp
US	35.244.159.8:443	eu-u.openx.net	udp
US	52.7.91.107:443	sync.1rx.io	tcp
DE	18.153.64.118:443	match.sharethrough.com	tcp
US	8.8.8.8:53	cs.media.net	udp
US	8.8.8.8:53	cs.media.net	udp
US	35.227.244.76:443	cs.media.net	tcp
US	8.8.8.8:53	yahoo-match.dotomi.com	udp
US	8.8.8.8:53	yahoo-match.dotomi.com	udp
NL	89.207.16.204:443	yahoo-match.dotomi.com	tcp
US	8.8.8.8:53	tpsc-ew1.doubleverify.com	udp
US	8.8.8.8:53	tpsc-ew1.doubleverify.com	udp
US	130.211.44.5:443	tpsc-ew1.doubleverify.com	tcp
US	8.8.8.8:53	sync.go.sonobi.com	udp
US	8.8.8.8:53	sync.go.sonobi.com	udp
US	69.166.1.67:443	sync.go.sonobi.com	tcp
US	69.166.1.67:443	sync.go.sonobi.com	tcp
US	8.8.8.8:53	p.rfihub.com	udp
US	8.8.8.8:53	p.rfihub.com	udp
US	8.8.8.8:53	pixel-sync.sitescout.com	udp
US	8.8.8.8:53	pixel-sync.sitescout.com	udp
US	8.8.8.8:53	cs.krushmedia.com	udp
US	8.8.8.8:53	cs.krushmedia.com	udp
US	8.8.8.8:53	sync.mathtag.com	udp
US	8.8.8.8:53	sync.mathtag.com	udp
US	8.8.8.8:53	fei.pro-market.net	udp
US	8.8.8.8:53	fei.pro-market.net	udp
US	8.8.8.8:53	d.turn.com	udp
US	8.8.8.8:53	d.turn.com	udp
IE	52.94.223.37:443	aax-eu.amazon-adsystem.com	tcp
US	8.8.8.8:53	dpm.demdex.net	udp
US	8.8.8.8:53	dpm.demdex.net	udp
NL	193.0.160.131:443	p.rfihub.com	tcp
US	34.36.216.150:443	pixel-sync.sitescout.com	tcp
US	80.77.82.130:443	cs.krushmedia.com	tcp
US	74.121.140.211:443	sync.mathtag.com	tcp
US	104.26.5.241:443	fei.pro-market.net	tcp
NL	46.228.164.30:443	d.turn.com	tcp
IE	52.16.129.226:443	dpm.demdex.net	tcp
US	8.8.8.8:53	cm.mgid.com	udp
US	104.17.199.65:443	cm.mgid.com	udp
US	8.8.8.8:53	capi.connatix.com	udp
US	8.8.8.8:53	capi.connatix.com	udp
US	104.18.41.104:443	capi.connatix.com	udp
US	34.36.216.150:443	pixel-sync.sitescout.com	udp
US	130.211.44.5:443	tpsc-ew1.doubleverify.com	tcp
US	34.238.229.121:443	sync.1rx.io	tcp
US	13.248.245.213:443	eb2.3lift.com	tcp
GB	23.214.208.27:443	hbx.media.net	tcp
US	130.211.44.5:443	tpsc-ew1.doubleverify.com	tcp
US	8.8.8.8:53	tpc.googlesyndication.com	udp
US	8.8.8.8:53	tpc.googlesyndication.com	udp
GB	142.250.140.132:443	tpc.googlesyndication.com	tcp
GB	142.250.129.104:443	www.google.com	tcp
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	150.171.28.11:443	edge.microsoft.com	tcp
US	130.211.44.5:443	tpsc-ew1.doubleverify.com	tcp
US	130.211.44.5:443	tpsc-ew1.doubleverify.com	tcp

US	216.239.34.36:443	region1.google-analytics.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.28.11:443	edge.microsoft.com	tcp
GB	92.123.128.159:443	www.bing.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	150.171.27.11:443	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	13.107.246.64:443	api.edgeoffer.microsoft.com	tcp
US	8.8.8.8:53	buymeacoffee.com	udp
US	8.8.8.8:53	buymeacoffee.com	udp
US	104.26.3.199:443	buymeacoffee.com	udp
US	8.8.8.8:53	cdn.buymeacoffee.com	udp
US	8.8.8.8:53	cdn.buymeacoffee.com	udp
US	104.26.3.199:443	cdn.buymeacoffee.com	udp
US	8.8.8.8:53	connect.facebook.net	udp
US	8.8.8.8:53	connect.facebook.net	udp
NL	57.144.222.128:443	connect.facebook.net	udp
US	8.8.8.8:53	www.google.com	udp
US	8.8.8.8:53	www.google.com	udp
US	8.8.8.8:53	static.ads-twitter.com	udp
US	8.8.8.8:53	plausible.io	udp
US	8.8.8.8:53	plausible.io	udp
US	8.8.8.8:53	cdn-cookieyes.com	udp
US	8.8.8.8:53	cdn-cookieyes.com	udp
US	8.8.8.8:53	analytics.ahrefs.com	udp
US	8.8.8.8:53	analytics.ahrefs.com	udp
GB	142.250.129.106:443	www.google.com	udp
GB	151.101.188.157:443	static.ads-twitter.com	tcp
GB	143.244.38.136:443	plausible.io	tcp
US	104.18.39.141:443	analytics.ahrefs.com	udp
US	104.18.18.62:443	cdn-cookieyes.com	tcp
GB	142.250.129.106:443	www.google.com	tcp
US	104.18.39.141:443	analytics.ahrefs.com	tcp
US	8.8.8.8:53	edge.microsoft.com	udp
US	8.8.8.8:53	edge.microsoft.com	udp
US	150.171.27.11:443	edge.microsoft.com	tcp
US	8.8.8.8:53	js.stripe.com	udp
US	8.8.8.8:53	js.stripe.com	udp
US	8.8.8.8:53	app.buymeacoffee.com	udp
US	8.8.8.8:53	app.buymeacoffee.com	udp
US	3.175.86.93:443	js.stripe.com	tcp
US	104.26.2.199:443	app.buymeacoffee.com	udp
GB	143.244.38.136:443	plausible.io	tcp
US	8.8.8.8:53	log.cookieyes.com	udp
US	8.8.8.8:53	log.cookieyes.com	udp
US	104.20.23.25:443	log.cookieyes.com	udp
US	8.8.8.8:53	www.google.co.uk	udp
US	8.8.8.8:53	www.google.co.uk	udp
US	8.8.8.8:53	region1.analytics.google.com	udp
US	8.8.8.8:53	region1.analytics.google.com	udp
US	8.8.8.8:53	stats.g.doubleclick.net	udp
US	8.8.8.8:53	stats.g.doubleclick.net	udp
US	8.8.8.8:53	googleads.g.doubleclick.net	udp
US	8.8.8.8:53	googleads.g.doubleclick.net	udp
US	216.239.32.36:443	region1.analytics.google.com	tcp
US	172.217.76.156:443	stats.g.doubleclick.net	tcp
GB	142.250.117.155:443	googleads.g.doubleclick.net	udp
GB	142.250.151.94:443	www.google.co.uk	udp
US	8.8.8.8:53	t.co	udp
US	8.8.8.8:53	t.co	udp
US	8.8.8.8:53	analytics.twitter.com	udp
US	8.8.8.8:53	analytics.twitter.com	udp

US	104.18.18.62:443	cdn-cookieyes.com	tcp
US	162.159.140.229:443	analytics.twitter.com	tcp
US	162.159.140.229:443	analytics.twitter.com	tcp
US	8.8.8.8:53	directory.cookieyes.com	udp
US	8.8.8.8:53	directory.cookieyes.com	udp
US	166.117.105.37:443	directory.cookieyes.com	tcp
US	8.8.8.8:53	js.stripe.com	udp
US	8.8.8.8:53	js.stripe.com	udp
US	151.101.64.176:443	js.stripe.com	tcp
US	151.101.64.176:443	js.stripe.com	tcp
US	151.101.64.176:443	js.stripe.com	udp
US	8.8.8.8:53	m.stripe.network	udp
US	8.8.8.8:53	m.stripe.network	udp
FR	3.174.255.72:443	m.stripe.network	tcp
FR	3.174.255.72:443	m.stripe.network	tcp
US	8.8.8.8:53	m.stripe.com	udp
US	8.8.8.8:53	m.stripe.com	udp
US	35.85.193.243:443	m.stripe.com	tcp
US	216.239.32.36:443	region1.analytics.google.com	udp
US	172.217.76.156:443	stats.g.doubleclick.net	udp
US	8.8.8.8:53	www.facebook.com	udp
US	8.8.8.8:53	www.facebook.com	udp
GB	57.144.240.1:443	www.facebook.com	udp

5. 6. Files

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Africa\Conakry

MD5	09a9397080948b96d97819d636775e33
SHA1	5cc9b028b5bd2222200e20091a18868ea62c4f18
SHA256	d2efac4e5f23d88c95d72c1db42807170f52f43dd98a205af5a92a91b9f2d997
SHA512	2eccf2515599ed261e96da3fbcfbab0b6a2dfc86a1d87e3814091709f0bfe2f600c3044c8555ed027978a8ae9045666ee639a8c249f48d665d8e5c60f0597799

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Africa\Djibouti

MD5	86dcc322e421bc8bdd14925e9d61cd6c
SHA1	289d1fb5a419107bc1d23a84a9e06ad3f9ee8403
SHA256	c89b2e253a8926a6cecf7eff34e4bfcdb7fe24daff22d84718c30deec0ea4968
SHA512	d32771be8629fb3186723c8971f06c3803d31389438b29bf6baa958b3f9db9a38971019583ba272c7a8f5eb4a633dfc467bfcb6f76faa8e290bad4fd7366bb2b

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Africa\Kigali

MD5	b07064beada5be6289ed9485ecc9733d
SHA1	b0ff96d087e4c86adb55b851c0d3800dfbb05e9a
SHA256	444ed3a710414bc6bf43eb27e591da49d3be3db153449a6a0c9473f7e39fdbcb
SHA512	0ce1322f4a6f6568cdf61fc699eead4147015829650e90d791c223b45f3a23ead720ff41b4c8cc10ee915175e052d4740347a4454d23c18a3c57d30ded5a904c

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Africa\Lagos

MD5	8244c4cc8508425b6612fa24df71e603
SHA1	30ba925b4670235915dddfa1dd824dd9d7295eac
SHA256	cffeb0282ccbd7fba0e493ff8677a1e5a6dd5197885042e437f95a773f844846
SHA512	560c7581dcb2c800eae779005e41406beaf15d24efc763304e3111b9bb6074fe0ba59c48b5a2c5511245551b94418bbc35934d9bd46313fcc6e383323056668c

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\America\Curacao

MD5	adf95d436701b9774205f9315ec6e4a4
SHA1	fcf8be5296496a5dd3a7a97ed331b0bb5c861450
SHA256	8491e557ff801a8306516b8ca5946ff5f2e6821af31477eb47d7d191cc5a6497
SHA512	f8fceff3c346224d693315af1ab12433eb046415200abaa6cdd65fd0ad40673fdddf67b83563d351e4aa520565881a4226fb37d578d3ba88a135e596ebb9b348

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\America\Toronto

MD5	8dabdbbb4e33dcb0683c8a2db78fedc4
SHA1	a6d038ecff7126ee19ebb08a40d157c9a79964cd
SHA256	a587a1a1607439f7bac283e1815f2bdbafb9649a453d18e06c2e44e6996d888f
SHA512	35bfd5182535f5257d7ee693eb6827751993915129d7f3cc276783926b1f4db7a00d8f0b44a95ac80c294a9cc1b84bda6418134c2a5c10ba6c89946bd8ef97a3

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\EST

MD5	0972a9c4c28bf71eeab5f0bac573cdbc
SHA1	a94fbc2d567e41723f03629b6c9a864260108a17
SHA256	91ac80fe976931c490d058c8ce8b5d71ffa6d4961f6ca13ea9c153f0b0bccea0
SHA512	ece548f7d840a588523aacddc93891e0dd300390f79de063e60074e00a92ae33a8201642b841ff868387f1ac2188c485cce941d83c7a3617d27ac286dbcc0c17

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Etc\Greenwich

MD5	9cd2aef183c064f630dfcf6018551374
SHA1	2a8483df5c2809f1dfe0c595102c474874338379
SHA256	6d9f378883c079f86c0387a5547a92c449869d806e07de10084ab04f0249018d
SHA512	dafa0cb9d0a8e0ff75a19be499751ad85372aafa856ff06dd68ecf2b1c5578bb98a040becaecf0aed2c3e4ff7372ff200fe7614334756d19fe79dd61c01d4e92

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Europe\London

MD5	a40006ee580ef0a4b6a7b925fee2e11f
SHA1	1beba7108ea93c7111dabc9d7f4e4bfdea383992
SHA256	c85495070dca42687df6a1c3ee780a27cbcb82f1844750ea6f642833a44d29b4
SHA512	316ecacc34136294ce11dcb6d0f292570ad0515f799fd59fbff5e7121799860b1347d802b6439a291f029573a3715e043009e2c1d5275f38957be9e04f92e62e

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Europe\Oslo

MD5	7db6c3e5031eaf69e6d1e5583ab2e870
SHA1	918341ad71f9d3acd28997326e42d5b00fba41e0
SHA256	5ee475f71a0fc1a32faeb849f8c39c6e7aa66d6d41ec742b97b3a7436b3b0701
SHA512	688eaa6d3001192addaa49d4e15f57aa59f3dd9dc511c063aa2687f36ffd28ffef01d937547926be6477bba8352a8006e8295ee77690be935f76d977c3ea12fe

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Europe\Skopje

MD5	6213fc0a706f93af6ff6a831fecbc095
SHA1	961a2223fd1573ab344930109fbd905336175c5f
SHA256	3a95adb06156044fd2fa662841c0268c2b5af47c1b19000d9d299563d387093a
SHA512	8149de3fd09f8e0f5a388f546ffe8823bdcda662d3e285b5cebc92738f0c6548ccb6ed2a5d086fd738cb3edc8e9e1f81c5e2e48edb0571e7ea7f131675b99327

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\MET

MD5	355f0d3e2a3ee15ea78526f5eeb0cf7d
SHA1	d90f3247c4716c2e1068d5ad9c88ca2091bec4e8
SHA256	812f55aeb6e8cde9ddf4786e15eb4256b21e82cf5f5d28da1bad17d94570cac0
SHA512	96a5fa48a15167e55ffad5b0241c90caeb7f0433ad62dd43463a4c52c25c59f7357681cb586fc52e812e8173adc12cec9eff66d27d5f41e19d55f6c1fce12937

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\PRC

MD5	09dd479d2f22832ce98c27c4db7ab97c
SHA1	79360e38e040eaa15b6e880296c1d1531f537b6f
SHA256	64ffc2e43a94435a043c040d1d3af7e92d031adc78e7737af1861baa4eeef3e6
SHA512	f88ae25f3f04c7d5d5f98aafecc03cc7e4e56f1cd4c8deba6afd043f0fb7fe67b4d50e4df5493e77c6b34ba183e019442e736a13f784ba8c2847c06fd74ff200

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Pacific\Yap

MD5	ec972f59902432836f93737f75c5116f
SHA1	331542d6faf6ab15ffd364d57fbaa62629b52b94
SHA256	9c1dfa1c15994dd8774e53f40cb14dcf529143468721f1dba7b2c2e14ae9f5f0
SHA512	e8e8c8f6d096c352d1244280254e4c6ecf93f7c2ff69ecc6fa4363a6be8a2daf6cfcd7f0d96bc2669268ced5565532fa06be348a139b0742ccccb83953c6324d

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\Pacific\Wallis

MD5	5bdd7374e21e3df324a5b3d178179715
SHA1	244ed7d52bc39d915e1f860727ecfe3f4b1ae121
SHA256	53268a8a6b11f0b8e02fc67683ae48d074efaf7b4c66e036c1478107afd9a7d7
SHA512	9c76f39e8795c50e6c5b384a7ff1f308a1c5173f42f810759b36cdeae7d33d1dac4934efeed580c59d988c152e2d7f8d9b8eb2073ab1fc15e4b9c10900c7b383

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\UCT

MD5	38bb24ba4d742dd6f50c1cba29cd966a
SHA1	d0b8991654116e9395714102c41d858c1454b3bd
SHA256	8b85846791ab2c8a5463c83a5be3c043e2570d7448434d41398969ed47e3e6f2
SHA512	194867d0cf66c2de4969dbfeb58c775964ecb2132acdc1b000b5ef0998cefde4a2979ffc04ec8b7dcb430e43326a79d9cedb28ecea184345aa7d742eaf9234ac

C:\Users\Admin\AppData\Local\Temp_MEI42042\pytz\zoneinfo\US\Mountain

MD5	648f67a7744849f2ca07f4d5871e9021
SHA1	faa7d6cf4178d032d8ba8a4d77eac0fd47f8a718
SHA256	32e819c00a43b3c348f539d700d425504f20b8d068c16418d26fa9b693e775c9
SHA512	3dab6d6a04a4856cba78ef499f1a436f1f71b1dea494ee098b76c1702531108ae0a1d7b6de05e9d9315027624b790e084d69b25507738099f6026cd2a9559f31

C:\Users\Admin\AppData\Local\Temp_MEI42042\ucrtbase.dll

MD5	286b308df8012a5dfc4276fb16dd9ccc
SHA1	8ae9df813b281c2bd7a81de1e4e9cef8934a9120
SHA256	2e5fb14b7bf8540278f3614a12f0226e56a7cc9e64b81cbd976c6fcf2f71cbfb
SHA512	24166cc1477cde129a9ab5b71075a6d935eb6eebcae9b39c0a106c5394ded31af3d93f6dea147120243f7790d0a0c625a690fd76177dddab2d2685105c3eb7b2

C:\Users\Admin\AppData\Local\Temp_MEI42042\python311.dll

MD5	387bb2c1e40bde1517f06b46313766be
SHA1	601f83ef61c7699652dec17edd5a45d6c20786c4
SHA256	0817a2a657a24c0d5fbb60df56960f42fc66b3039d522ec952dab83e2d869364
SHA512	521cde6eaa5d4a2e0ef6bbfdea50b00750ae022c1c7bd66b20654c035552b49c9d2fac18ef503bbd136a7a307bdeb97f759d45c25228a0bf0c37739b6e897bad

C:\Users\Admin\AppData\Local\Temp_MEI42042\VCRUNTIME140.dll

MD5	be8dbe2dc77ebe7f88f910c61aec691a
SHA1	a19f08bb2b1c1de5bb61daf9f2304531321e0e40
SHA256	4d292623516f65c80482081e62d5dadb759dc16e851de5db24c3cbb57b87db83
SHA512	0da644472b374f1da449a06623983d0477405b5229e386accadb154b43b8b083ee89f07c3f04d2c0c7501ead99ad95aecaa5873ff34c5eeb833285b598d5a655

C:\Users\Admin\AppData\Local\Temp_MEI42042\base_library.zip

MD5	99ada859f99e907452d98b7911f3cf34
SHA1	a23d5e35eb36ab369dc4b2ebf0ea263e1014e93a
SHA256	2b573c891e17cc325aa944d67d7d020ac32dfb58400c256dbd4fe61e2bde8c59
SHA512	5ebd57e9305463f95046ca2dd5dc71155331fa026cd648a7f9b6c51938ee6ed4b8080bbe24c5a08dfbd75269962da0dc3111698b7f6eebb876e51a3b709f2e87

C:\Users\Admin\AppData\Local\Temp_MEI42042_ctypes.pyd

MD5	565d011ce1cee4d48e722c7421300090
SHA1	9dc300e04e5e0075de4c0205be2e8aae2064ae19
SHA256	c148292328f0aab7863af82f54f613961e7cb95b7215f7a81cafaf45bd4c42b7
SHA512	5af370884b5f82903fd93b566791a22e5b0cded7f743e6524880ea0c41ee73037b71df0be9f07d3224c733b076bec3be756e7e77f9e7ed5c2dd9505f35b0e4f5

C:\Users\Admin\AppData\Local\Temp_MEI42042\python3.DLL

MD5	7e07c63636a01df77cd31cfca9a5c745
SHA1	593765bc1729fdca66dd45bbb6ea9fcd882f42a6
SHA256	db84bc052cfb121fe4db36242ba5f1d2c031b600ef5d8d752cf25b7c02b6bac6
SHA512	8c538625be972481c495c7271398993cfe188e2f0a71d38fb51eb18b62467205fe3944def156d0ff09a145670af375d2fc974c6b18313fa275ce6b420decc729

C:\Users\Admin\AppData\Local\Temp_MEI42042\libffi-8.dll

MD5	0f8e4992ca92baaf54cc0b43aaccce21
SHA1	c7300975df267b1d6adcbac0ac93fd7b1ab49bd2
SHA256	eff52743773eb550fcc6ce3efc37c85724502233b6b002a35496d828bd7b280a
SHA512	6e1b223462dc124279bfca74fd2c66fe18b368ffbca540c84e82e0f5bcbea0e10cc243975574fa95ace437b9d8b03a446ed5ee0c9b1b094147cefaf704dfe978

C:\Users\Admin\AppData\Local\Temp_MEI42042\pyexpat.pyd

MD5	79561bc9f70383f8ae073802a321adfb
SHA1	5f378f47888e5092598c20c56827419d9f480fa7
SHA256	c7c7564f7f874fb660a46384980a2cf28bc3e245ca83628a197ccf861eab5560
SHA512	476c839f544b730c5b133e2ae08112144cac07b6dfb8332535058f5cbf54ce7ed4a72efb38e6d56007ae755694b05e81e247d0a10210c993376484a057f2217c

C:\Users\Admin\AppData\Local\Temp_MEI42042\tk86t.dll

MD5	50be514d4234103d49fb2a600a272fce
SHA1	e441b77a421598998d24814afd4af8090d306e57
SHA256	b6af038120f2b8644c7ce1e11917f410009848287622135d7e386f90d28a831c
SHA512	d93467b688f68f15eb46dc1aef4bd4f4d0b91193a2c40a1d4b5cc6e906a443343e261225df530527491a01c58803b91a138d5147d7a02aedeb9cddd3adc77fef

C:\Users\Admin\AppData\Local\Temp_MEI42042\tcl86t.dll

MD5	50be441afc42714cb7fe98677f304807
SHA1	0604a2992f698e45d1524c44a924b7451d8ad003
SHA256	4e699ff2d6d147d0586c8c77be5a18f20ca0758f432d7b0f489223f2fa4dd221
SHA512	a99c7b5c9d42c53cf51ace16871bb2f1dfc9424077b0a758ec1b8583eb1be3cdd413d005188fa82dd61093b56882cd72b32f15b55599c5f0fcbce34321afb639

C:\Users\Admin\AppData\Local\Temp_MEI42042\libssl-3.dll

MD5	19a2aba25456181d5fb572d88ac0e73e
SHA1	656ca8cdfc9c3a6379536e2027e93408851483db
SHA256	2e9fbcd8f7fdc13a5179533239811456554f2b3aa2fb10e1b17be0df81c79006
SHA512	df17dc8a882363a6c5a1b78ba3cf448437d1118ccc4a6275cc7681551b13c1a4e0f94e30ffb94c3530b688b62bff1c03e57c2c185a7df2bf3e5737a06e114337

C:\Users\Admin\AppData\Local\Temp_MEI42042\libcrypto-3.dll

MD5	e547cf6d296a88f5b1c352c116df7c0c
SHA1	cafa14e0367f7c13ad140fd556f10f320a039783
SHA256	05fe080eab7fc535c51e10c1bd76a2f3e6217f9c91a25034774588881c3f99de
SHA512	9f42edf04c7af350a00fa4fdf92b8e2e6f47ab9d2d41491985b20cd0adde4f694253399f6a88f4bdd765c4f49792f25fb01e84ec03fd5d0be8bb61773d77d74d

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-utility-l1-1-0.dll

MD5	708a5bc205384633a7b6674eecc7f0f0
SHA1	01603a7826029293236c67fce02ace8d392a0514
SHA256	d8ba5f17b9ffcbf3aeaf3fa1da226832d2fa90f81acce0cd669464e76ce434ac
SHA512	8638845326ab6543338baa7a644af8be33a123e1fc9da2037158be7c8d165691ccd06cb3ff73696a30b8801eab030e81f93db81216bb3b7e83a320a0df5af270

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-time-l1-1-0.dll

MD5	fccce207a34c947f01d3f23a7dd09569
SHA1	75f722801c77285db98a08af763252a0255e99e2
SHA256	7c7f6393f06de11750adb09cc5698ae55cd9fb27b2e51e207286feb1b5b2b156
SHA512	d3d923f133594eb4325f4a6e5ed46fcc348a7c0f310f14eaa38c6fad070ba637bdb4a77200feb231114e111d07a86595a6130291028cde3a284d9f847ec38ad4

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-string-l1-1-0.dll

MD5	639b1fb35cb61ba633eb1791b750631f
SHA1	392a6925009f5fb02a4c122c9ce31d82b9059628
SHA256	25b8f83a7767211b11132775a0e27a45aa4ec8ab4e6572599f9c172ae3606b40
SHA512	def547ef66673862cea9bb13c433edce24a3075c328d9b3b9452f2f01f2f4243daab38c0f8571c52d601bc4aecaaa0682dbebf6be41cae345787a719063ebf58

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-stdio-l1-1-0.dll

MD5	ef37235fc43157a4c93241d5e49e304b
SHA1	d4de26b36812c2ddccd1618b4d7ac02ad1b42273
SHA256	a9c5a153d8c0286f9b41a2b1c65854ad9e6471b8755b7de87bae4470e60bcab6
SHA512	c0857760d5d069beeb1eb1737f4160530910331bf6047022836cf58137bd28c2a966a8760a681859f57ebd810fd424ce231402eddde1316eaef7b6f9f773afbb

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-runtime-l1-1-0.dll

MD5	bbaa58e9e1abdf7d8c4c69652d29d789
SHA1	38aef13abc14502354e8c5c3c37b97a8e2e5fdcf
SHA256	c5902934d026d7e15fbe9917d474f3322846a41a25e66f4b2b1f758801879f4b
SHA512	7882a8e1e1ea7e217f70ff9df27d36709b4be23588909ef002f3eb1b9a7d3eea2591a8524af2c83448ddfff0911658517c6989683245c54678583f359a78b0ad

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-process-l1-1-0.dll

MD5	9d6925407136753e8eb8234d59fa3f1f
SHA1	62631b7007d394fb4d406ea686b291fff9e486cd
SHA256	f6156b1020380ec4f0e48577ebedaaef5fb1ab1f337d8b4e72e6a33a7567a9cc
SHA512	ab04de62524e465810cd0ee81e85018863e276d49861e67a920667af802e94869b816b47a6e3c4738179a7a7d726d44bbba6e47d9097363a63eaff51cd56de8a

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-private-l1-1-0.dll

MD5	c830c6447e6de3d6a611702c591831e3
SHA1	2b5a0a8702c769eeaaf101852456aa3ecf3914e3
SHA256	1bc82bed6143d2bf1b6b08a7809f4a5e29317d6fddd338a7da3c0223522e4bbf
SHA512	9ad2b9fd4792632714394f0dc293776484d16b1efbaba2daf1816df911a58fe4a920c48059b44848681b7a266a0ea036ec36ee0a031f52c034a15ad74d3bdb51

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-math-l1-1-0.dll

MD5	aa9624cb27cc50a3fbbd3b223a617b1c
SHA1	797aea1c5cedd1125276bfc5dcd7a3fb8c6355aa
SHA256	606d66d82db562ea7979179d06486a0f94d079941d26b80a1e2c49d29959df6f
SHA512	024975e6787f7a6b0ab6e4b02ad33901f8473b97dc73d4f03b7a116b24ac74150c0c48990ea7a4fb750f9fe728dafed172796743f802e70f2150eefcf70fe96a

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-locale-l1-1-0.dll

MD5	09796dab12cbbd920f632aeb89820193
SHA1	7d81c0e5537b6d8b79af0c28cd102e064027c78d
SHA256	bd14c67ea28e21d6257ad780a37122c9b5773f69e693f5db6bffaee4d839526e
SHA512	09a6175dccbbd18a62209e156089f1167dfb8040c97c8c2c14724ce2a8fbe6ce039d7fe04fb8bd60092427beb7fdd8e7127d611f006fff1cf2a1ad75e9e5ef3a

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-heap-l1-1-0.dll

MD5	527bbbfded529ea77ee798d94ce0f243
SHA1	647f8c89eb4db3cf3656292b3de984b32c6e02a5
SHA256	bab9ac3ec83e380ae51e4295ef3bf2c738627812d3a49d1e713661abbc8dc57a
SHA512	c1ed69e15ab19084390cf9d1ceab791758ac4ddd688169f3b814b0e4cf1fc3b6ba17651e35b25dcdc601a8a64821d58933d52a5e939942fa134dfd04fca04c8b

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-filesystem-l1-1-0.dll

MD5	47555752931cecf90e796499b62ec729
SHA1	217b171764fba5e91190d1f8a36feccb3f6d4585
SHA256	9a9e2a65a281644e368d0f272b95ba5f6b445d1c35910d06056c5ebeb77402db
SHA512	a68009f0306d4d8e70951978d2c184eb80fbec98c6db0997bd7b0b503dd63019363cfef68a9adbfb568c0a552b774fbdbeb1bcf45f211a6a3224b49e85a5619c

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-environment-l1-1-0.dll

MD5	e93c7f013493b12ad40229b19db02ce6
SHA1	ef878bfbfd2f8328bbb8cff1aa29a39e624a8503
SHA256	17d63275d00bdd8670422b95bd264c532998e0a1b041079e54fce4b6b7a55819
SHA512	2f4a25ea4062840bea10442cad665a72abbce747307ad9ce7b3bb89eaf7dcc28f1e9396749576be304fd793690ddc445653613440442695e72b761eacacb6020

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-convert-l1-1-0.dll

MD5	3560176d0cdbe2f5d33f543348e0a027
SHA1	1e35a1f7793fc3899927835491f28fe5b903edcd
SHA256	ebb2ae5535a64f65daeab8235585114fc9dd2cf1a49f5852d446250b998b6ae4
SHA512	8ab24c8c9fe8331f21be96818c5fa69ae5578eb742c4504596310bb0db7c4c087d350fa47a13ed9ff2e051bb62ac5581de082d0177923d24fee6b140afecf50b

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-crt-conio-l1-1-0.dll

MD5	5794b8e183eb547aadd5faf30a8c4dd2
SHA1	5b1ed8a9da14d8ecc4209662809727931aa49307
SHA256	b762061b688aae679afe788904d2c9970f74a7dac98f3b42463d08f25e483d3f
SHA512	3e896854e5dd957ab2b88c82fbaf2eaa03729bab30fd8518bd999081f4da9000d9b22894b324e5930df161c7adaec3fc87fd00de60dcda34876007aea4a2fd31

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-util-l1-1-0.dll

MD5	3c58a804b90a0782e80bbbf6c6b6f167
SHA1	b333143e0f6e508b51d27adf7872b586fa54c794
SHA256	6eda016742a6171205a387a14b3c0b331841567740376f56768f8c151724207d
SHA512	773f8deded48b34babe24d955a501f4f357c20125affb6eade36ce6a7acd380906713c366318f79d627747e636d156875c216fffac26dba25373bbc1c820da76

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-timezone-l1-1-0.dll

MD5	43d8d2fb8801c5bd90d9482ddf3ea356
SHA1	d582b55cd58531e726141c63ba9910ff185d72e0
SHA256	33f4fddc181066fce06b2227bded813f95e94ed1f3d785e982c6b6b56c510c57
SHA512	0e073381a340db3f95165dbcceb8dfbf1ed1b4343e860446032400a7b321b7922c42ee5d9a881e28e69a3f55d56d63663adb9bb5abb69c5306efbf116cc5e456

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-sysinfo-l1-2-0.dll

MD5	fc9fc5f308ffc2d2d71814df8e2ae107
SHA1	24d7477f2a7dc2610eb701ed683108cd57eca966
SHA256	2703635d835396afd0f138d7c73751afe7e33a24f4225d08c1690b0a371932c0
SHA512	490fa6dc846e11c94cfe2f80a781c1bd1943cddd861d8907de8f05d9dc7a6364a777c6988c58059e435ac7e5d523218a597b2e9c69c9c34c50d82cac4400fe01

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-sysinfo-l1-1-0.dll

MD5	b65bf5ef316880fd8d21e1b34eb5c8a9
SHA1	3ab4674cb5c76e261fe042d6d0da8a20bfcbcbae
SHA256	b203d862ddef1dd62bf623fc866c7f7a9c317c1c2ae30d1f52cb41f955b5698e
SHA512	4af3b0ef9a813ce1a93a35dd6869817910ae4b628f374477f60ea1831d2cc1aae7908262672e11954a4953bdff22bcc5fe23b4a736788e8e5ef4f8ac30eb24f8

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-synch-l1-2-0.dll

MD5	8f107a7bc018227b181a0e7e76e9ca39
SHA1	ef57e24f29d2b1deeacefd82171873b971a3f606
SHA256	efc1e4460984a73cf47a3def033af1c8f3b1dbc1a56cd27781d3aacf3e3330cb
SHA512	d8d8250aaf93fa99e9d1e4286b32579de0029c83867a787c0a765505a0f8cbd2dd076bb324509d5c4867423bc7dc8f00c8b8458e08e8cbfa8dd731d03dd1ae3f

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-synch-l1-1-0.dll

MD5	436ea0237ed040513ec887046418faaa
SHA1	44bafbbdb1b97d86505e16b8a5fcb42b2b771f91
SHA256	3a72b4f29f39a265d32ad12f0ce15dbf60129c840e10d84d427829ede45e78ad
SHA512	9f0dbfb538c05383ae9abfe95e55740530ecc12c1890d8862deacbc84212be0740d82afc9e81d529125221e00b2286cae0d4b3ca8dd3a6c57774d59f37933692

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-string-l1-1-0.dll

MD5	28005b20fbef6e1db10912d0fdd6471c
SHA1	47b83697677e08e4ebcff6fc41eca7ece120cc17
SHA256	60fc31d2a0c634412f529dba76af3b9bf991352877c6dae528186d3935704cfd
SHA512	45d6f860d7f7aefaa7a0a3b4b21b5c3234f442e39d6259e0a9e2083890533c275f07ddda93fddc7445928a55475b83c63253d3b08e41e5576f9029b205dfb36a

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-rtlsupport-l1-1-0.dll

MD5	3c5c7a3130b075b2def5c413c127173f
SHA1	f3d2b8ad93f3dc99c8410d34c871aec56c52e317
SHA256	9dc1e91e71c7c054854bd1487cb4e6946d82c9f463430f1c4e8d1471005172b1
SHA512	46a52631e3dd49b0ae10afbdf50a08d6d6575f3093b3921b2fa744704e2d317f8b10a6d48ad7f922a7843731782521773032a6cc04833b00bd85e404c168ffe4

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-profile-l1-1-0.dll

MD5	7a629293eeb0bca5f9bdee8ade477c54
SHA1	a25bf8bac4fbfd9216ea827e71344ba07b1d463b
SHA256	7809160932f44e59b021699f5bc68799eb7293ee1fa926d6fcca3c3445302e61
SHA512	1c58c547d1fe9b54ddf07e5407edaf3375c6425ca357aa81d09c76a001376c43487476a6f18c891065ab99680501b0f43a16a10ed8e0d5e87b9a9542098f45fe

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-processthreads-l1-1-1.dll

MD5	385f562bdc391ccd4f81aca3719f3236
SHA1	f6633e1dac227ba3cd14d004748ef0c1c4135e67
SHA256	4ad565a8ba3ef0ea8ab87221ad11f83ee0bc844ce236607958406663b407333e
SHA512	b72ed1a02d4a02791ca5490b35f7e2cb6cb988e4899eda78134a34fb28964ea573d3289b69d5db1aac2289d1f24fd0a432b8187f7ae8147656d38691ae923f27

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-processthreads-l1-1-0.dll

MD5	c123f2c161884fbff4f00ef1e1391266
SHA1	7db3055da53916bea2b85b159491a0772fb620ce
SHA256	5ccb89e93d67bc3288d4e84649c5346e66e15e3d7cd65d989daf3f4cb584be9a
SHA512	dac5616320b9052254b5687959e67126c4a938e79173d8245675a9651674384c36cc856f996ef88ae621ec67afc66166266575 85d92bb5d14602a7cc9fc0f669

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-processenvironment-l1-1-0.dll

MD5	7fd4a71085783ccfe9c289c07bcf9b04
SHA1	bb6ffdb5c069dbba06998dc877d24f72dad6298d
SHA256	c4eca98c3c67b6395d5b005b00ac1eb0318b86b23aa71035a44c2b1602befba9
SHA512	a96c5b90b8384b239be111d90caa3b947651ad73382ab9e5dbe4a4b6ad30921876545331d37c8d5a8f669e39d71bf60983c4ba39c479e23015c2f7579c5e55cd

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-namedpipe-l1-1-0.dll

MD5	4a28ca64f44b91f43945ee3971e0996a
SHA1	45b3d8584c58e8d6ae507fdbd772feeb1886c8b0
SHA256	c05f1fffe3b5a2738ea54ce9485cca026fb9635f982626fba1e1dcc531897273
SHA512	862a0428f08d447cd1ee0431969e0fbcb182f4c46418c26d26fa33e586e686d9c093c1ca5781f544ce9276195ce973850719636e39e465f059607f455ecfdd93

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-memory-l1-1-0.dll

MD5	8d285430e8bda6d5c9b683579adcb180
SHA1	619dbbcff06c659e3fc48f03917a4dadbfc1c275
SHA256	0512a35316ec9180437f86696a84c5c06a7e4e82e050055a656e5bf9fca206f9
SHA512	38405dd85dd62f843abb55acea1b64d7d63bb601445bf1b32078cde5bbef4861dd99f26659281fe2aea86f58cfb1725d8c63d91fb539dcbf5d98cdbe783337fc

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-localization-l1-2-0.dll

MD5	5241df2e95e31e73ccfd6357ad309df0
SHA1	2644cc5e86dfad1ad2140181ab2ca79725f95411
SHA256	6ee44dd0d8510dc024c9f7c79b1b9fa88c987b26b6beb6653ddd11751c34e5dc
SHA512	52cccd1dd237e764e34996c0c5f7a759a7f0eff29b61befeaf96a16d80df2ba9ee2c3615f875153198a145d68f275aea6d02187e6eee5a129e3e2ab81aaceb16

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-libraryloader-l1-1-0.dll

MD5	5fbcb20d99e463259b4f15429010b9cd
SHA1	b16770f8bb53dc2bafcb309824d6fa7b57044d8a
SHA256	7f39ba298b41e4963047341288cab36b6a241835ee11ba4ad70f44dacd40906c
SHA512	7ba1ac34b3ecfbfb8252f5875be381d8ef823b50dfe0e070222175ee51191f5ee6d541eeedd1445ed603a23d200ce9ce15914c8ed3fafe7e7f3591f51f896c58

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-kernel32-legacy-l1-1-1.dll

MD5	0c1cc0a54d4b38885e1b250b40a34a84
SHA1	24400f712bbe1dd260ed407d1eb24c35dcb2ecac
SHA256	a9b13a1cd1b8c19b0c6b4afcd5bb0dd29c0e2288231ac9e6db8510094ce68ba6
SHA512	71674e7ed8650cac26b6f11a05bfc12bd7332588d21cf81d827c1d22df5730a13c1e6b3ba797573bb05b3138f8d46091402e63c059650c7e33208d50973dde39

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-interlocked-l1-1-0.dll

MD5	86023497fa48ca2c7705d3f90b76ebc5
SHA1	835215d7954e57d33d9b34d8850e8dc82f6d09e8
SHA256	53b25e753ca785bf8b695d89dde5818a318890211dc992a89146f16658f0b606
SHA512	8f8370f4c0b27779d18529164fa40cbfddafa81a4300d9273713b13428d0367d50583271ea388d43c1a96fed5893448cd14711d5312da9dfa09b9893df333186

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-heap-l1-1-0.dll

MD5	344a09b4be069f86356a89482c156647
SHA1	2506ffeb157cb531195dd04d11d07c16e4429530
SHA256	8f105771b236dbcb859de271f0a6822ce1cb79c36988dd42c9e3f6f55c5f7eb9
SHA512	4c1e616443576dc83200a4f98d122065926f23212b6647b601470806151ff15ea44996364674821afec492b29ba868f188a9d6119b1e1d378a268f1584ca5b29

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-handle-l1-1-0.dll

MD5	416aa8314222db6cbb3760856be13d46
SHA1	5f28fe2d565378c033ef8eea874bc38f4b205327
SHA256	39095f59c41d76ec81bb2723d646fde4c148e7cc3402f4980d2ade95cb9c84f9
SHA512	b16ed31dc3343caea47c771326810c040a082e0ab65d9ae69946498ceb6ae0dee0a570dbcd88090668a100b952c1ff88bade148811b913c90931aa0e657cd808

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-file-l2-1-0.dll

MD5	e368a236f5676a3da44e76870cd691c9
SHA1	e4f1d2c6f714a47f0dc29021855c632ef98b0a74
SHA256	93c624b366ba16c643fc8933070a26f03b073ad0cf7f80173266d67536c61989
SHA512	f5126498a8b65ab20afaaf6b0f179ab5286810384d44638c35f3779f37e288a51c28bed3c3f8125d51feb2a0909329f3b21273cb33b3c30728b87318480a9ef8

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-file-l1-2-0.dll

MD5	cc228ff8d86b608e73026b1e9960b2f8
SHA1	cef0705aee1e8702589524879a49e859505d6fe0
SHA256	4cadbc0c39da7c6722206fdcebd670abe5b8d261e7b041dd94f9397a89d1990d
SHA512	17abd9e0ec20b7eb686e3c0f41b043d0742ab7f9501a423b2d2922d44af660379792d1cc6221effbd7e856575d5babf72657ae9127c87cc5cf678bd2ceb1228f

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-file-l1-1-0.dll

MD5	9f45a47ebfd9d0629f4935764243dd5a
SHA1	86a4a0ea205e31fb73f3bfcce24945bd6bea06c7
SHA256	1ca895aba4e7435563a6b43e85eba67a0f8c74aa6a6a94d0fc48fa35535e2585
SHA512	8c1cdcad557bff1685a633d181fcf14ec512d322caeaeb9c937da8794c74694fe93528fc9578cb75098f50a2489ed4a5dedf8c8c2ac93eeb9c8f50e3dd690d5f

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-fibers-l1-1-1.dll

MD5	050a30a687e7a2fa6f086a0db89aa131
SHA1	1484322caaf0d71cbb873a2b87bdd8d456da1a3b
SHA256	fc9d86cec621383eab636ebc87ddd3f5c19a3cb2a33d97be112c051d0b275429
SHA512	07a15aa3b0830f857b9b9ffeb57b6593ae40847a146c5041d38be9ce3410f58caa091a7d5671cc1bc7285b51d4547e3004cf0e634ae51fe3da0051e54d8759e1

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-fibers-l1-1-0.dll

MD5	b5e2760c5a46dbeb8ae18c75f335707e
SHA1	e71db44fc0e0c125de90a9a87ccb1461e72a9030
SHA256	91d249d7bc0e38ef6bcb17158b1fdc6dd8888dc086615c9b8b750b87e52a5fb3
SHA512	c3400772d501c5356f873d96b95dc33428a34b6fcaad83234b6782b5f4bf087121e4fd84885b1abab202066da98eb424f93dd2eed19a0e2a9f6ff4a5cfd1e4f3

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-errorhandling-l1-1-0.dll

MD5	c2f8c03ecce9941492bfbe4b82f7d2d5
SHA1	909c66c6dfea5e0c74d3892d980918251bb08632
SHA256	d56ce7b1cd76108ad6c137326ec694a14c99d48c3d7b0ace8c3ff4d9bcee3ce8
SHA512	7c6c85e390bbe903265574e0e7a074da2ce30d9376d7a91a121a3e0b1a8b0fffd5579f404d91836525d4400d2760cb74c9cb448f8c5ae9713385329612b074cf

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-debug-l1-1-0.dll

MD5	226a5983ae2cbbf0c1bda85d65948abc
SHA1	d0f131dcba0f0717c5dea4a9ca7f2e2ecf0ad1c3
SHA256	591358eb4d1531e9563ee0813e4301c552ce364c912ce684d16576eabf195dc3
SHA512	a1e6671091bd5b2f83bfaa8fcf47093026e354563f84559bd2b57d6e9fa1671eea27b4ed8493e9fdf4bde814074dc669de047b4272b2d14b4f928d25c4be819d

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-datetime-l1-1-0.dll

MD5	8f8eb9cb9e78e3a611bc8acaec4399cb
SHA1	237eee6e6e0705c4be7b0ef716b6a4136bf4e8a8
SHA256	1bd81dfd19204b44662510d9054852fb77c9f25c1088d647881c9b976cc16818
SHA512	5b10404cdc29e9fc612a0111b0b22f41d78e9a694631f48f186bdde940c477c88f202377e887b05d914108b9be531e6790f8f56e6f03273ab964209d83a60596

C:\Users\Admin\AppData\Local\Temp_MEI42042\api-ms-win-core-console-l1-1-0.dll

MD5	9f746f4f7d845f063fea3c37dcebc27c
SHA1	24d00523770127a5705fcc2a165731723df36312
SHA256	88ace577a9c51061cb7d1a36babbbefa48212fadc838ffde98fdfff60de18386
SHA512	306952418b095e5cf139372a7e684062d05b2209e41d74798a20d7819efeb41d9a53dc864cb62cc927a98df45f7365f32b72ec9b17ba1aee63e2bf4e1d61a6e4

C:\Users\Admin\AppData\Local\Temp_MEI42042\sqlite3.dll

MD5	89c2845bd090082406649f337c0cca62
SHA1	956736454f9c9e1e3d629c87d2c330f0a4443ae9
SHA256	314bba62f4a1628b986afc94c09dc29cdaf08210eae469440fbf46bcdb86d3fd
SHA512	1c467a7a3d325f0febb0c6a7f8f7ce49e4f9e3c4514e613352ef7705a338be5e448c351a47da2fb80bf5fc3d37dbd69e31c935e7ff58ead06b2155a893728a82

C:\Users\Admin\AppData\Local\Temp_MEI42042\select.pyd

MD5	e4ab524f78a4cf31099b43b35d2faec3
SHA1	a9702669ef49b3a043ca5550383826d075167291
SHA256	bae0974390945520eb99ab32486c6a964691f8f4a028ac408d98fa8fb0db7d90
SHA512	5fccfb3523c87ad5ab2cde4b9c104649c613388bc35b6561517ae573d3324f9191dd53c0f118b9808ba2907440cbc92aecfc77d0512ef81534e970118294cdee

memory/3076-1835-0x00007FFB7D5F0000-0x00007FFB7E96E000-memory.dmp

C:\Users\Admin\AppData\Local\Temp__PSScriptPolicyTest_sr5xjjbp.ohi.ps1

MD5	d17fe0a3f47be24a6453e9ef58c94641
SHA1	6ab83620379fc69f80c0242105ddffd7d98d5d9d
SHA256	96ad1146eb96877eab5942ae0736b82d8b5e2039a80d3d6932665c1a4c87dcf7
SHA512	5b592e58f26c264604f98f6aa12860758ce606d1c63220736cf0c779e4e18e3cec8706930a16c38b20161754d1017d1657d35258e58ca22b18f5b232880dec82

C:\Users\Admin\AppData\Local\Temp\radar_historia_v43.json

MD5	de3af228b926427836766d8f9b7ac779
SHA1	0f2cdd097b4867b4a50eb95de15f351b20775241
SHA256	d0dce83e0d75e35f2019648e135a90a23f72607fad7d0779fb206f8ece8de354
SHA512	12774eda1b19e87722fb8b5aedef0e13c37a7be2bfd95086b84084e35a0796eb3491dfef391ecb1c1ee960e5b59644a975dc9047e7e171cd8cd221448f204959

memory/3224-1852-0x000001A76B170000-0x000001A76B192000-memory.dmp

memory/6028-1888-0x0000013E46E20000-0x0000013E46E28000-memory.dmp

memory/6028-1887-0x0000013E46E10000-0x0000013E46E1A000-memory.dmp

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

MD5	667300793dcb45c09297144209c23c32
SHA1	46b8735b6d665e0973cec41104bfc9ad460e8fb1
SHA256	6470fed5075d1ab3ad140cad016720b7705022b2b82e26500b6f90b10d81a426
SHA512	489ae59e69f02c2110ddb45bec5d7065ad58e33d67e9a3b4b4d8a8f4cbf0a9865466b11abcf7694af4055d4c7b2677cddf9fdeba22c1e6d3dc5079a70d693b6c

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

MD5	a4bd39276f6a7063da79fb76decb5271
SHA1	3d0150f2cb357ba2c9ee676ae0b78d38d5f22722
SHA256	6d159e2d0fd9bec377afb7e7681719c083bba3719227b86de9301df1dfd5bd95
SHA512	d6e90bf18213618a6fa94ae6e2521afed5bdacae6c2acce9cca3537ab32d9b7b7f46e3f65abf1ed3a2df677ae1df0b213b448bafe0a52d2bedad93bf5d14ed25

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

MD5	7255671cf8108f6173f8b192dc01c012
SHA1	8488509dc2c6ef4047cf918c98a34ba7730d93dc
SHA256	69426451cae50925bb586e921d42d130a6d98a5b6fd62cfc80829c26d282cc2d
SHA512	6676544585e876c1869a117564057f26143fb1f7caeaeac0af6f38e2ae54df9d5683feea4ccea8873855d543f591aad13076fe25b71895ac1db26a5e5c4f23b8

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\TokenBroker\Cache\5a2a7058cf8d1e56c20e6b19a7c48eb2386d141b.tbres

MD5	9cf3e495d6c69994f6000222a23d4bdf
SHA1	c45c6d7510fe02ef0a88aad0be3b93a784823354
SHA256	623f8e8d3aa739c5976be2e83e082f3a8acc3c2045c0793a40e70339642dd04d
SHA512	d2e883b0e254f07efafcc332450f5587c19ba4e7ec5dd3925b21608028daf907b87f37584fe7a839f06fc6042635fe61f5e9082fb1a5714a4138ee379100ffcb

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

MD5	b705718ae4bbdd148710bf502e539ffe
SHA1	d0be9829a912e74b7af2d4ba191914f149ce337f
SHA256	0aabff75f1ccb2319e7a018fb6a278380e29aea0f212e8ebae08c61eda598434
SHA512	bb289fc60ff226a2bcf400087a8181148dbd9c653c26f596289b53bc6e454aa7fdeeaa6d179ca378b0d8436a1c00794557a20c4ccbff0120ff2e5ac514d08165

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\BookmarkMergedSurfaceOrdering

MD5	377d072e137022223a370760763420bb
SHA1	534e5f914ae99bf0a342a2f7a7e0724bd0d11ef7
SHA256	4489f9e3e454748b3521eb214e0a5694d562cff3d9ff511cb456953c8f534c00
SHA512	d1e37e45e8d603c46c9254d7295744104222b09340246c5e5f50d661d4688ccc2068adf1e0cd78599bcdcf475f8a0a6255dcd3e429812aa14cc2e2022309955c

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

MD5	902622d177776fafc9f85d74f2ab73b8
SHA1	deb767db94129ecffdcd2ff94970687033409107
SHA256	84ab2d00a9c76d63c3edf4fd0139236f6b94e49bd7889e4f5f63f19941bc1ed1
SHA512	d219535bf4fd4b1561c34b2e0c9f3938de8a86a85aba4d19f31b413483d01cb6afe611077620907839f4340475f1468c2097318751aeef4a61c64a75751aea2e

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

MD5	d9253f3f50271d1852f6ff6cdf92d8b6
SHA1	b818bd74c8a968675d4b4b4381ce30870da3390e
SHA256	76e9af61874fdf2ad58ddc00147a46b7043307c412b06be2041a07671fe6f3e1
SHA512	659b614c153c8baee53dc531d7be4ba49db829af1353e2300a5130af3ea514253d1580b04ca255ba9dac103fb2569b4e9844f230477d2a1e1edb7cd57dcb136c

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

MD5	835f05f7ca9c9c7ce2cfbbe945c3f242
SHA1	f42150dcafa3f8fda1f004c265d2a20112b5520c
SHA256	6fb8d8767a63e15b016d063124ce7ff6ece07bdc04c05f194a5f0bfa66216aac
SHA512	a45fa59cb7ead70f544b9ee3ac1f4c70cdfa11a5634e7ac6db41c0be62b2537fe5835a0eb67bada9b76a022d01fcafde9ff91f592858a7f7f12825366814f1dd

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

MD5	6a51a88bd3a158d3848392748077d871
SHA1	51dcc43d773f15a75aa82b2c74c3a957a35b636e
SHA256	c7cffb5504088ac2710f596198823cdd2bb3fb7b597f758332a92ad3e23c1960
SHA512	2d6523bf1f7313ec441069d6a87cbe709f7064272b2c262a9e1888531ed8d455b61ff489d862138ca8748cd17d322919ff74962247ab58c4a741e5b0d8e20da0

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

MD5	079385445bae610056cb4b6d868af994
SHA1	d3122df47e5547d65276e3541b2105a3a1daf0ec
SHA256	4ec6e8f41adbad234f7f1d292f265acfaad48aefa1312a9fe641efe6877fd2fb
SHA512	1e3935e55717e190f19977efd4a4019eeea126b7473cb1a2f14ee82a5c077a12e7ada0d23a516bf033077088d99adfa2b7f77adde8253b59aa3d1ac22eedb09a

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

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

memory/5824-2398-0x000001B9E8200000-0x000001B9E83E4000-memory.dmp

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

MD5	90ffe58a25b1562c210fa833ab682e8e
SHA1	c2bf5d2e5de53f233a09c6a525021d4fb607abcc
SHA256	f8fa505cbd93d76615b669c910f2f17aad1d7d8700922d275aaadd3cd956768e
SHA512	578793aa9d5897b48bf31156d70b88b5ece5424bcb80fd829d9cdb994b3d63b898253f87e052f117d693765709301849f37372f39ff27347b64d41c7fa910c2d

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

MD5	edab2094062c5d2b353bb558bb77d161
SHA1	3f641e371d2ac2de14be114aaff08bab7bac4336
SHA256	b3d8186b2b817d79a8d63228f405572b01ad281d349ce59321f08c7a9a2da1cb
SHA512	20363bde687af3251851f6075b1083d3784c808ad91467c6de13154fa383060c22f15c9a2bc4bc7954c4d3141c9f7a45e1bede37527fbc21ba59d92158386f4b

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

MD5	5e7981ec30b7f57e86cc9f7f422eddd1
SHA1	e6c111b903cfb10a0ac1118c7703362bd509cca8
SHA256	1276a886756696a75e0e730cf103e97a0df8a18976c8c5dc6a49ae55906ed65c
SHA512	4f616550ad7a0c70e1482522ffa62350b866951a1d2db0c1ea7f71a82272394c05af1d7284a8777ed52807b8a516dc7b6ad06d023ac5c5a05e7117ff443da6d5

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

MD5	bdb69641cbebf698536aaaaf74f070b1
SHA1	5e9e74d054e3d3f1d6b4f9b21973b086ff3e1c8e
SHA256	b060b8b5800a02b4868cf9df1702f7323f5fbddce3f3239691099b4859ce1f44
SHA512	c2f9164d4f24504e6e12a40d3851e105db274fad9b1179a3a98a5b829a01c4ea972bf51d5e07826e07668561ef670b6b2c2ea9af0c7c4f0eb463cee91853824f

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\index-dir\the-real-index

MD5	13d59a25fa8accb99fa138f6cc13fc6b
SHA1	f731744a85939059b91479f94bdfe77cf13ce7f2
SHA256	31761e22dfdd6dd741a595a98284f84cea25096e17071a5734bf9f61dc905a93
SHA512	8657694d2295f0d402333df62b30df190c69eae176de489c2931f6353990aa77fa4b6510aff9bd78310f8ac520f84d66f0c373cb265fbc19b91b88a2ce7b3e48

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

MD5	5b71e6ade379eca8b8c4ce07d970e2a6
SHA1	f45d42f6a6dc872f80a38dae63379699d1aadee2
SHA256	b7f98bee352e6333978adbaac7c1fdbcd80343f1fde1c0a6d95b1a39f8ee6715
SHA512	32336ecb205160c9faf9e2594b035ab76606c6239e825ac657425956dec736e589188a0176bcf9f3b90b29020422361a6ba66826995e82e0e0836f92564b799c

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

MD5	80272ffbf6c6d774e517e86afdeab59e
SHA1	b0b75f5bfc63933565e86ad021699f582c2b36d1
SHA256	bcdb1e80d6c9c473389099df61a8e6a084f4ac027f80eace9450dbbdbbe33226
SHA512	f076335589cbea83cd845a4af843d36a476550c9c1417f89ed58f1dff1c9fe700fabe1ac3acf313e6349081c43ea28c2d0219c1ee983cf4b5c2ef9e893a00ed7

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\ShaderCache\data_1

MD5	d2012b8a8d95d3763dfefd545cbcda73
SHA1	0e6224424e7941ab9130c64122aac879246320f7
SHA256	8bcc2b6dc79379700b2e24eaf12bc3e2677d960b2fe1a3cab88f627acd79756f
SHA512	a021f898f69652f38387e37ff90c2facd66617468b3bc548611b655f5f9b787243f3e9b8a9a5906ca6f39a66af83e22caba94ad8a3be50f736e8d7769ab17736

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

MD5	6f32737d481bd45fea7a9c7070e9b81a
SHA1	eaa0c0d3a45113eca732131697dd9e0e5c0a9d1d
SHA256	10f34c5d2fa612d17750f9e0edecfb688d66bbdc8393b59d1dc8484bac5847fd
SHA512	225a45171ee131f7e730422b78b91fc2c249343f223f9d3a58699ec8fed00375456ae374ceaa464181bd083783a3beab99e5687dca83fc2768b5db2fb2780762

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

MD5	09cf80500552e6954600e807940ab1b9
SHA1	d7b2319ab0f2f1342d4d91d6e718b28cddb9f004
SHA256	1ca9af0b806809c04a6d3c46f8383baaf80691fb31a9ee310deaef8445a1c3d7
SHA512	83430c0d3585a67a3802ecf27207898bc34ef9a3f475afddd2fb3d2f5fc2a1605b3ddc9f8d2eef0080d0905c4a16ec9324a0be14e2f5e8685dcf0dfda5f35d41

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

MD5	08ac108b45da24326c4ce48e08c01097
SHA1	8066f27c8cb28ffe3e2f9f9eb0f01c3d8fea277a
SHA256	fb94815a483b90c093b0b3946d7b45ece1a68b47bd8a3240987e2f33672a568f
SHA512	ed989518eec1fb804c8de2ff7e2e2fbb2c84bd1131eb38fcaf5cccee9b99df3b14220dd97a2ae01c76fc9852c187269c0235685412b86faeb0d6c56bcac81cc6

memory/6476-2952-0x0000022CB3600000-0x0000022CB37E4000-memory.dmp

C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\AdPlatform\auto_show_data.db\000001.dbtmp

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

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

MD5	d496ebe4f9e51ca21f8f003f21fab09c
SHA1	6384760a741990b754e0ee185b871964d5d8287b
SHA256	fb69c149f0fb4bbe50fa9d77b1337f24cd059ee04359729fc6a768c6c89b676e
SHA512	02825ad63a140e87ef17f666b28c0882f5d47ef5b47a010560fde471ff8057b4c35a71f141441d1670e8fee5fc7bcd184db017f93f30f009ab4a2b46da7e9e15