Nov 26 2023

NETMANAGEIT

Intelligence Report

ParaSiteSnatcher How Malicious Chrome Extensions Target Brazil

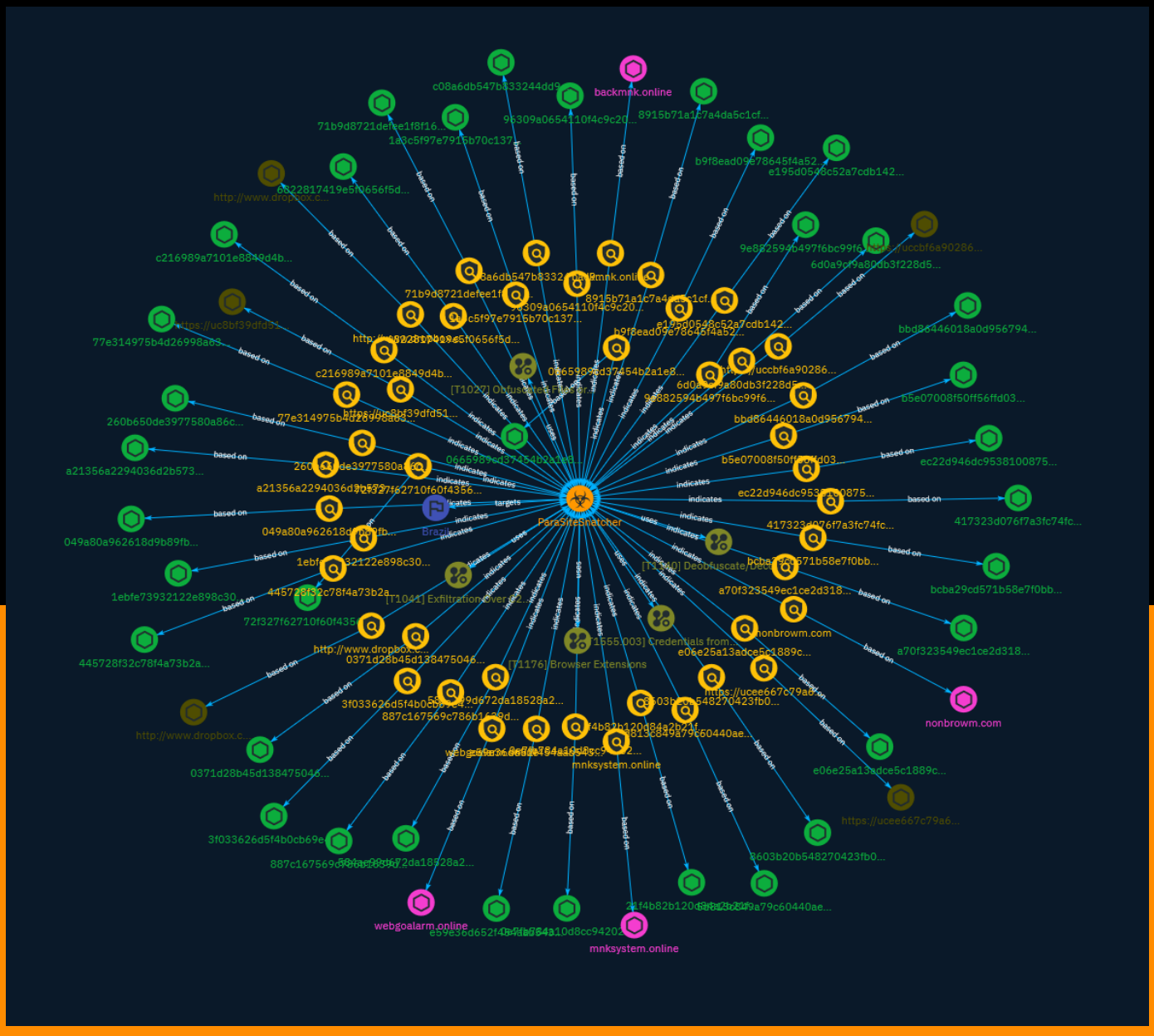

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The ParaSiteSnatcher framework allows threat actors to monitor, manipulate, and exfiltrate highly sensitive information from multiple sources. ParaSiteSnatcher also utilizes the powerful Chrome Browser API to intercept and exfiltrate all POST requests containing sensitive account and financial information before the HTTP request initiates a transmission control protocol (TCP) connection.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name

Credentials from Web Browsers

ID

T1555.003

Description

Adversaries may acquire credentials from web browsers by reading files specific to the target browser.(Citation: Talos Olympic Destroyer 2018) Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers. For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, `AppData\Local\Google\Chrome\User Data\Default\Login Data` and executing a SQL query: `SELECT action_url, username_value, password_value FROM logins;`. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function `CryptUnprotectData`, which uses the victim's cached logon credentials as the decryption key.(Citation: Microsoft CryptUnprotectData April 2018) Adversaries have executed similar procedures for common web browsers such as FireFox, Safari, Edge, etc. (Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017) Windows stores Internet Explorer and Microsoft Edge credentials in Credential Lockers managed by the [Windows Credential Manager](https://attack.mitre.org/techniques/T1555/004). Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mimikittenz July 2016) After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases

where credentials gained from web browsers overlap with privileged accounts (e.g. domain administrator).

Name

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Indicator

Name
e59e36d652f454aab543722501ac23258d295ef0f1ecf7c97cad7720ceee6123
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'e59e36d652f454aab543722501ac23258d295ef0f1ecf7c97cad7720ceee6123']
Name
72f327f62710f60f43569741c2cb391b833b44c4dafe1f5d5c085a39c485b5df
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '72f327f62710f60f43569741c2cb391b833b44c4dafe1f5d5c085a39c485b5df']
Name

https://ucee667c79a6c55d864febd411be.dl.dropboxusercontent.com/cd/0/get/CGJ3qwC1u0jLr4CMzA6xZ77B9wEwh0nsM6QbQmwau3W0r-QUrhwEOFMEtcKTaPiNvaz-wngORZmw9w_Bc0ljndJu1OFJJa-1qoI66JNdBmu8fa9dNvM64fbOYZohfqjDQpHDQbkFXU7ffTWOXkk8ZlEk/file?dl=1

Pattern Type

stix

Pattern

[url:value = 'https://ucee667c79a6c55d864febd411be.dl.dropboxusercontent.com/cd/0/get/CGJ3qwC1u0jLr4CMzA6xZ77B9wEwh0nsM6QbQmwau3W0r-QUrhwEOFMEtcKTaPiNvaz-wngORZmw9w_Bc0ljndJu1OFJJa-1qoI66JNdBmu8fa9dNvM64fbOYZohfqjDQpHDQbkFXU7ffTWOXkk8ZlEk/file?dl=1']

Name

584ae99d672da18528a2c4d6c0506a83b55503a650ea1aafd5419f62afcee761

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '584ae99d672da18528a2c4d6c0506a83b55503a650ea1aafd5419f62afcee761']

Name

9e882594b497f6bc99f6da26211c54d5005064423b1f93059406332e36ae3eba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9e882594b497f6bc99f6da26211c54d5005064423b1f93059406332e36ae3eba']

Name

887c167569c786b1639d87e0f624ce4af939baf67e1113bedde7226c744dbb38

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '887c167569c786b1639d87e0f624ce4af939baf67e1113bedde7226c744dbb38']

Name

http://www.dropbox.com/scl/fi/cx975utps1os4gw38q73b/1698022264.zip?rlkey=tqmsmhjonobx8ise21lp35601&dl=1

Pattern Type

stix

Pattern

[url:value = 'http://www.dropbox.com/scl/fi/cx975utps1os4gw38q73b/1698022264.zip?rlkey=tqmsmhjonobx8ise21lp35601&dl=1']

Name

417323d076f7a3fc74fcb1534e39a7c55b6c9cb2a27120369634fd1c32d60f94

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '417323d076f7a3fc74fcb1534e39a7c55b6c9cb2a27120369634fd1c32d60f94']

Name

http://www.dropbox.com/scl/fi/8otjw9dhf4kpb7s5vzxdu/1698746809.zip?rlkey=1w2k81ure5hm9ut5owezxa2gg&dl=1

Pattern Type

stix

Pattern

[url:value = 'http://www.dropbox.com/scl/fi/8otjw9dhf4kpb7s5vzxdu/1698746809.zip?rlkey=1w2k81ure5hm9ut5owezxa2gg&dl=1']

Name

c08a6db547b833244dd93aca9441059efe65428c588f0db591bcc8157fe4b43f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c08a6db547b833244dd93aca9441059efe65428c588f0db591bcc8157fe4b43f']

Name

21f4b82b120d84a2b21f95d75a583f36d7116cc3768785a3d0f213b50e86b240

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '21f4b82b120d84a2b21f95d75a583f36d7116cc3768785a3d0f213b50e86b240']

Name

c216989a7101e8849d4bd392377859c90772344289719519d5808ead81ae42e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c216989a7101e8849d4bd392377859c90772344289719519d5808ead81ae42e9']

Name

e195d0548c52a7cdb142c6c5acda2af40e350bd9d606ae4e1c03c6aa246572b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e195d0548c52a7cdb142c6c5acda2af40e350bd9d606ae4e1c03c6aa246572b3']

Name

0e7fb784a10d8cc942029477fee4c1b8907612e3f667970d5ca9fce885cac1d4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e7fb784a10d8cc942029477fee4c1b8907612e3f667970d5ca9fce885cac1d4']

Name

https://uccbf6a90286e6acc2a790729260.dl.dropboxusercontent.com/cd/0/get/CGqsvrqOuB4FhGVeZWMyQmSofO8uNJ8EV_sB9CypG92ekXY38jFAv9xQxx7QHpViLjUiEO7JzJ_eQurMhVA9ptRY0qTFFHQC0PkKvO64jHHju7RjYSIJo9vkJkoN7l5HPojdhpe-rLIy1U_oZboMSkgH/file?dl=1

Pattern Type

stix

Pattern

[url:value = 'https://uccbf6a90286e6acc2a790729260.dl.dropboxusercontent.com/cd/0/get/CGqsvrqOuB4FhGVeZWMyQmSofO8uNJ8EV_sB9CypG92ekXY38jFAv9xQxx7QHpViLjUiEO7JzJ_eQurMhVA9ptRY0qTFFHQC0PkKvO64jHHju7RjYSIJo9vkJkoN7l5HPojdhpe-rLIy1U_oZboMSkgH/file?dl=1']

Name

96309a0654110f4c9c20869b9f139c7aceea0d1f7f698892cdfd821f9463e04f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '96309a0654110f4c9c20869b9f139c7aceea0d1f7f698892cdfd821f9463e04f']

Name

1ebfe73932122e898c30098be4384a0fc9150565c3a340750b37b121ea7a55fa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ebfe73932122e898c30098be4384a0fc9150565c3a340750b37b121ea7a55fa']

Name

71b9d8721defee1f8f1694ce4e2ae8b1a99b78baa8e7fc9dd11364e97c390ff8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '71b9d8721defee1f8f1694ce4e2ae8b1a99b78baa8e7fc9dd11364e97c390ff8']

Name

5d813c849a79c60440ae2a36117e29da1da6c7649c00156b5cfe6222322e4cd6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5d813c849a79c60440ae2a36117e29da1da6c7649c00156b5cfe6222322e4cd6']

Name

77e314975b4d26998a6384c9cb0deda88b8fa5ea059e3fe7b48edd8a541f2315

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '77e314975b4d26998a6384c9cb0deda88b8fa5ea059e3fe7b48edd8a541f2315']

Name

b9f8ead09e78645f4a52290b88feafc899d3acf9db776259892058877bd9d250

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b9f8ead09e78645f4a52290b88feafc899d3acf9db776259892058877bd9d250']

Name

e06e25a13adce5c1889c613f12c269b4926f4900da155f4de5fedd46e45c5807

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e06e25a13adce5c1889c613f12c269b4926f4900da155f4de5fedd46e45c5807']

Name

0665989cd37454b2a1e83d0f930b471635fd993135facba20cc4c724682e64f1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0665989cd37454b2a1e83d0f930b471635fd993135facba20cc4c724682e64f1']

Name

nonbrowm.com

Pattern Type

stix

Pattern

[domain-name:value = 'nonbrowm.com']

Name

6822817419e5f0656f5d32cb1fcf2c03217ff7444e865d35e0d5405f3305b5a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6822817419e5f0656f5d32cb1fcf2c03217ff7444e865d35e0d5405f3305b5a6']

Name

ec22d946dc9538100875b86d2f6035f3541f5e3f08698304b9591efeea7d09a2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ec22d946dc9538100875b86d2f6035f3541f5e3f08698304b9591efeea7d09a2']

Name
mnksystem.online
Pattern Type
stix
Pattern
[domain-name:value = 'mnksystem.online']
Name
a21356a2294036d2b573e3f6350a198cd0c4e98d5c2e7ecc9d37089250a6c0c0
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a21356a2294036d2b573e3f6350a198cd0c4e98d5c2e7ecc9d37089250a6c0c0']
Name
bbd86446018a0d956794965a6b9f2da1402decb630f247529cd975a0cdfc3875
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'bbd86446018a0d956794965a6b9f2da1402decb630f247529cd975a0cdfc3875']

Name

445728f32c78f4a73b2a5c043aba674e5be14ffeb41a518fc774bbf4d7b408ba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '445728f32c78f4a73b2a5c043aba674e5be14ffeb41a518fc774bbf4d7b408ba']

Name

1a3c5f97e7915b70c1371dd9a0265565fe86f7f347e303e7a6d8eaad573d339b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a3c5f97e7915b70c1371dd9a0265565fe86f7f347e303e7a6d8eaad573d339b']

Name

a70f323549ec1ce2d31814a8f0852f23b62cade04011058c247a1e55ba049bfd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a70f323549ec1ce2d31814a8f0852f23b62cade04011058c247a1e55ba049bfd']

Name

260b650de3977580a86c63c7f13b0aaee606fe16feff552936eed8e3ad652627

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '260b650de3977580a86c63c7f13b0aaee606fe16feff552936eed8e3ad652627']

Name

8915b71a1c7a4da5c1cf73cdfa1d24c5546ed203e2a2d17f997ec31398bf85cc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8915b71a1c7a4da5c1cf73cdfa1d24c5546ed203e2a2d17f997ec31398bf85cc']

Name

webgoalarm.online

Pattern Type

stix

Pattern

[domain-name:value = 'webgoalarm.online']

Name

6d0a9cf9a80db3f228d51a8f078a6949bf96684cfb5f78f42a0941d070bc15e4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d0a9cf9a80db3f228d51a8f078a6949bf96684cfb5f78f42a0941d070bc15e4']

Name

bcba29cd571b58e7f0bbf9d72105e50f1eddf915207e9147c554b18922c5adf7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bcba29cd571b58e7f0bbf9d72105e50f1eddf915207e9147c554b18922c5adf7']

Name
3f033626d5f4b0cb69e4e902d80d1c3c4de647562e359a0d8904485799483e3b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3f033626d5f4b0cb69e4e902d80d1c3c4de647562e359a0d8904485799483e3b']
Name
b5e07008f50ff56ffd0389340a037da43b6398d57bf345dda3e0661098bf5ae4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b5e07008f50ff56ffd0389340a037da43b6398d57bf345dda3e0661098bf5ae4']
Name
8603b20b548270423fb03c2138c16f5f863ead4c48eb0999167df869e2eef8a6
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '8603b20b548270423fb03c2138c16f5f863ead4c48eb0999167df869e2eef8a6']

Name

049a80a962618d9b89fb0a2cf03ef2c3ee00975c5b424e209f073e3c7a491f2c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '049a80a962618d9b89fb0a2cf03ef2c3ee00975c5b424e209f073e3c7a491f2c']

Name

https://uc8bf39dfd51f19eca022ff937cc.dl.dropboxusercontent.com/cd/0/get/CGra8cbuRwTG62ccNRWQK3CHk96XzuTfm16q2nC1og5CiCXTPrwXZtf0TTJ3u6QelROuT3GllV05RL60fow_mvq9BpmNUeM0f6c1tUpdVEVYS3KaTHf-At7aLzI6ET-6MxKFT2NlOE9tgzXNEMIy3Ouy/file?dl=1

Pattern Type

stix

Pattern

[url:value = 'https://uc8bf39dfd51f19eca022ff937cc.dl.dropboxusercontent.com/cd/0/get/CGra8cbuRwTG62ccNRWQK3CHk96XzuTfm16q2nC1og5CiCXTPrwXZtf0TTJ3u6QelROuT3GllV05RL60fow_mvq9BpmNUeM0f6c1tUpdVEVYS3KaTHf-At7aLzI6ET-6MxKFT2NlOE9tgzXNEMIy3Ouy/file?dl=1']

Name

0371d28b45d13847504685a1baa360ce8e2e97301dfdc37de93f403b17484e98

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0371d28b45d13847504685a1baa360ce8e2e97301dfdc37de93f403b17484e98']

Name

backmnk.online

Pattern Type

stix

Pattern

[domain-name:value = 'backmnk.online']

Country

Name
Brazil

Malware

Name
ParaSiteSnatcher

Domain-Name

Value
nonbrowm.com
webgoalarm.online
backmnk.online
mnksystem.online

StixFile

Value
77e314975b4d26998a6384c9cb0deda88b8fa5ea059e3fe7b48edd8a541f2315
0e7fb784a10d8cc942029477fee4c1b8907612e3f667970d5ca9fce885cac1d4
260b650de3977580a86c63c7f13b0aaee606fe16feff552936eed8e3ad652627
1a3c5f97e7915b70c1371dd9a0265565fe86f7f347e303e7a6d8eaad573d339b
b9f8ead09e78645f4a52290b88feafc899d3acf9db776259892058877bd9d250
1ebfe73932122e898c30098be4384a0fc9150565c3a340750b37b121ea7a55fa
ec22d946dc9538100875b86d2f6035f3541f5e3f08698304b9591efeea7d09a2
bcba29cd571b58e7f0bbf9d72105e50f1eddf915207e9147c554b18922c5adf7
b5e07008f50ff56ffd0389340a037da43b6398d57bf345dda3e0661098bf5ae4
3f033626d5f4b0cb69e4e902d80d1c3c4de647562e359a0d8904485799483e3b
8915b71a1c7a4da5c1cf73cdfa1d24c5546ed203e2a2d17f997ec31398bf85cc
72f327f62710f60f43569741c2cb391b833b44c4dafe1f5d5c085a39c485b5df
21f4b82b120d84a2b21f95d75a583f36d7116cc3768785a3d0f213b50e86b240

e06e25a13adce5c1889c613f12c269b4926f4900da155f4de5fedd46e45c5807

9e882594b497f6bc99f6da26211c54d5005064423b1f93059406332e36ae3eba

96309a0654110f4c9c20869b9f139c7aceea0d1f7f698892cdfd821f9463e04f

6d0a9cf9a80db3f228d51a8f078a6949bf96684cfb5f78f42a0941d070bc15e4

e59e36d652f454aab543722501ac23258d295ef0f1ecf7c97cad7720ceee6123

c08a6db547b833244dd93aca9441059efe65428c588f0db591bcc8157fe4b43f

0665989cd37454b2a1e83d0f930b471635fd993135facba20cc4c724682e64f1

71b9d8721defee1f8f1694ce4e2ae8b1a99b78baa8e7fc9dd11364e97c390ff8

a70f323549ec1ce2d31814a8f0852f23b62cade04011058c247a1e55ba049bfd

5d813c849a79c60440ae2a36117e29da1da6c7649c00156b5cfe6222322e4cd6

445728f32c78f4a73b2a5c043aba674e5be14ffeb41a518fc774bbf4d7b408ba

417323d076f7a3fc74fcb1534e39a7c55b6c9cb2a27120369634fd1c32d60f94

0371d28b45d13847504685a1baa360ce8e2e97301dfdc37de93f403b17484e98

e195d0548c52a7cdb142c6c5acda2af40e350bd9d606ae4e1c03c6aa246572b3

049a80a962618d9b89fb0a2cf03ef2c3ee00975c5b424e209f073e3c7a491f2c

bbd86446018a0d956794965a6b9f2da1402decb630f247529cd975a0cdfc3875

584ae99d672da18528a2c4d6c0506a83b55503a650ea1aafd5419f62afcee761

a21356a2294036d2b573e3f6350a198cd0c4e98d5c2e7ecc9d37089250a6c0c0

c216989a7101e8849d4bd392377859c90772344289719519d5808ead81ae42e9

8603b20b548270423fb03c2138c16f5f863ead4c48eb0999167df869e2eef8a6

887c167569c786b1639d87e0f624ce4af939baf67e1113bedde7226c744dbb38

6822817419e5f0656f5d32cb1fcf2c03217ff7444e865d35e0d5405f3305b5a6

Url

Value
https://uc8bf39dfd51f19eca022ff937cc.dl.dropboxusercontent.com/cd/0/get/CGra8cbuRwTG62ccNRWQK3CHk96XzuTfm16q2nC1og5CiCXTPrwXZtf0TTJ3u6QelROuT3GllV05RL60fow_mvq9BpmNUeM0f6c1tUpdVEVYS3KaTHf-At7aLzI6ET-6MxKFT2NlOE9tgzXNEMIy3Ouy/file?dl=1
http://www.dropbox.com/scl/fi/cx975utps1os4gw38q73b/1698022264.zip?rlkey=tqmsmhjonobx8ise21lp35601&dl=1
https://ucee667c79a6c55d864febd411be.dl.dropboxusercontent.com/cd/0/get/CGJ3qwC1u0jLr4CMzA6xZ77B9wEwh0nsM6QbQmwau3W0r-QUrhwEOFMEtcKTaPiNvaz-wngORZmw9w_Bc0ljndJu1OFJJa-1qoI66JNdBmu8fa9dNvM64fbOYZohfqjDQpHDQbkFXU7ffTWOXkk8ZlEk/file?dl=1
http://www.dropbox.com/scl/fi/8otjw9dhf4kpb7s5vzxdu/1698746809.zip?rlkey=1w2k81ure5hm9ut5owezxa2gg&dl=1
https://uccbf6a90286e6acc2a790729260.dl.dropboxusercontent.com/cd/0/get/CGqsvrqOuB4FhGVeZWMyQmSofO8uNJ8EV_sB9CypG92ekXY38jFAv9xQxx7QHpViLjUiEO7JzJ_eQurMhVA9ptRY0qTFFHQC0PkKvO64jHHju7RjYSIJo9vkJkoN7l5HPojdhpe-rLIy1U_oZboMSkgH/file?dl=1

External References

- https://otx.alienvault.com/pulse/65607dfd5aa46bd47238155f
- https://www.trendmicro.com/en_us/research/23/k/parasitesnatcher-how-malicious-chrome-extensions-target-brazil-.html
- https://documents.trendmicro.com/assets/txt/20231121_ParaSiteSnatcher_IoCsl7nn42H.txt