Apr 01 2024

NETMANAGEIT

Intelligence Report Dissects infostealer malware

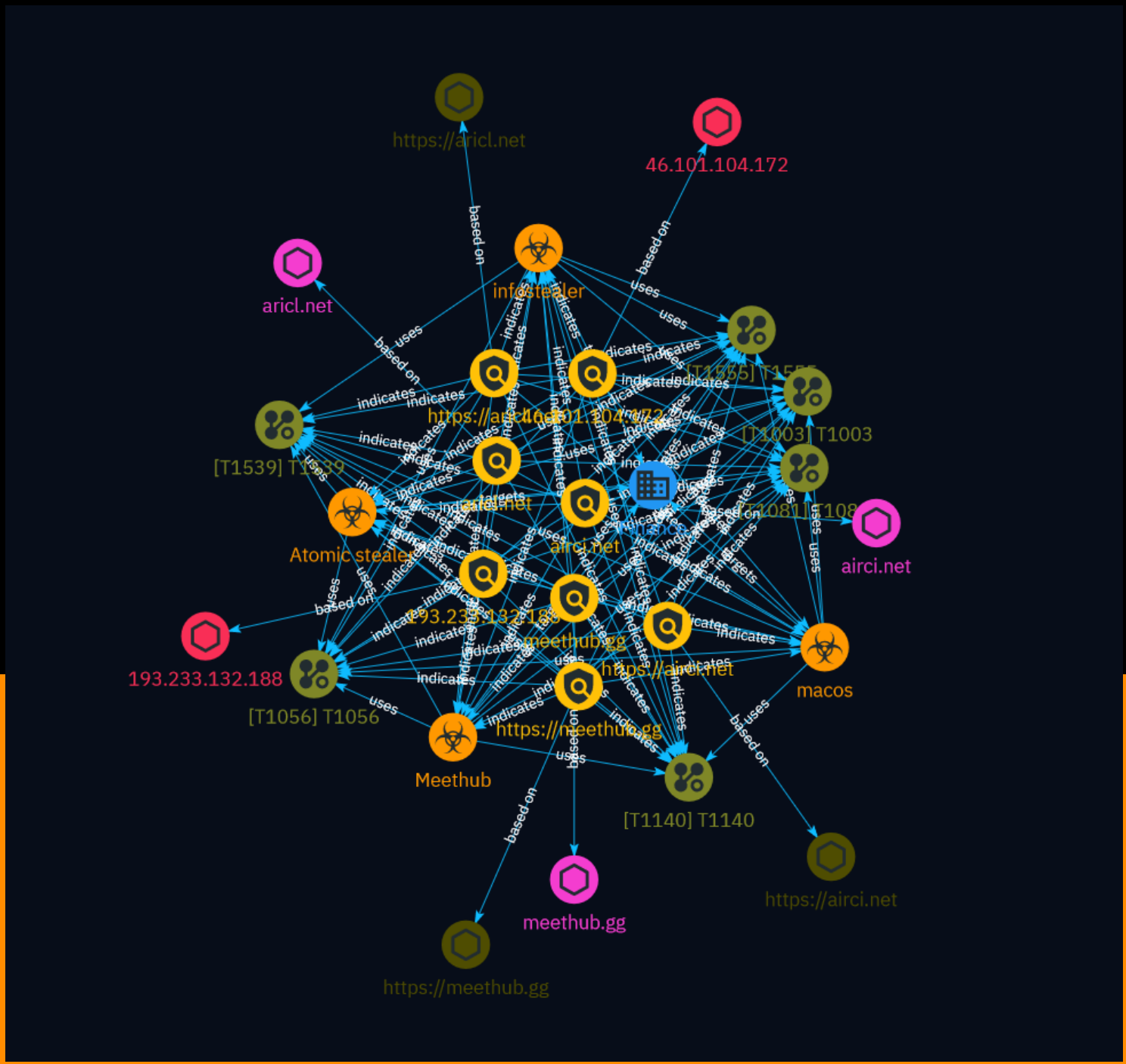

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Jamf Threat Labs analyzed two recent infostealer malware attacks targeting macOS users. The attacks used different techniques but had the common goal of stealing sensitive user data. The malware prompted for passwords, collected browser data, and exfiltrated information.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

meethub.gg

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** meethub.gg - **IPQS: IP Address:** 172.67.145.133

Pattern Type

stix

Pattern

[domain-name:value = 'meethub.gg']

Name

aricl.net

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5

days ago', 'timestamp': 1711557953, 'iso': '2024-03-27T12:45:53-04:00'} - **IPQS: Domain:** aricl.net - **IPQS: IP Address:** 104.21.93.64

Pattern Type

stix

Pattern

[domain-name:value = 'aricl.net']

Name

airci.net

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 weeks ago', 'timestamp': 1710700689, 'iso': '2024-03-17T14:38:09-04:00'} - **IPQS: Domain:** airci.net - **IPQS: IP Address:** 172.67.187.108

Pattern Type

stix

Pattern

[domain-name:value = 'airci.net']

Name

https://meethub.gg

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** meethub.gg - **IPQS: IP Address:** 172.67.145.133

Pattern Type

stix

Pattern

[url:value = 'https://meethub.gg']

Name

https://aricl.net

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 days ago', 'timestamp': 1711557953, 'iso': '2024-03-27T12:45:53-04:00'} - **IPQS: Domain:** aricl.net - **IPQS: IP Address:** 172.67.206.41

Pattern Type

stix

Pattern

[url:value = 'https://aricl.net']

Name

https://airci.net

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 weeks ago', 'timestamp': 1710700689, 'iso': '2024-03-17T14:38:09-04:00'} - **IPQS: Domain:** airci.net - **IPQS: IP Address:** 172.67.187.108

Pattern Type

stix

Pattern

[url:value = 'https://airci.net']

Name

193.233.132.188

Description

- **Zip Code:** N/A - **ISP:** Chromis It - **ASN:** 216319 - **Organization:** Chromis It - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 193.233.132.188 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Florida - **City:** Jacksonville - **Latitude:** 30.33 - **Longitude:** -81.66

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.233.132.188']

Name

46.101.104.172

Description

ISP: DigitalOcean, LLC **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLeYRBqiKjM4CWdBjyqLNMwN +gS7tnch7diPOfoaLFRd/ViSTG/Qx00fCye1DBol3dohQwMNj5ougzhX58jZp/8= Fingerprint: c7:c5:f2:25:9f:c9:cf:74:db:5c:9d:f4:f5:58:78:b7 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **8880:** ``` HTTP/1.1 404 Not Found X-Powered-By: Express Access-Control-Allow-Origin: * Content-Security-Policy: default-src 'none' X-Content-Type-Options: nosniff Content-Type: text/html; charset=utf-8 Content-Length: 139 Date: Sun, 31 Mar 2024 07:11:54 GMT Connection: keep-alive Keep-Alive: timeout=5

Cannot GET /

``` ----------

## Pattern Type

stix

## Pattern

[ipv4-addr:value = '46.101.104.172']
```

Malware

Name
Meethub
Name
infostealer
Name
macos
Name
Atomic stealer

Attack-Pattern

Name
T1081
ID
T1081
Name
T1056
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name

T1555

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name

T1140

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

T1539

ID

T1539

Description

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website. Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems. Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.(Citation: Pass The Cookie) There are several examples of malware targeting cookies from web browsers on the local system.(Citation: Kaspersky TajMahal April 2019)(Citation: Unit 42 Mac Crypto Cookies January 2019) There are also open source frameworks such as `Evilginx2` and `Muraena` that can gather session cookies through a malicious proxy (ex: [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)) that can be set up by an adversary and used in phishing campaigns.(Citation: Github evilginx2)(Citation: GitHub Mauraena) After an adversary acquires a valid cookie, they can then perform a [Web Session Cookie] (https://attack.mitre.org/techniques/T1550/004) technique to login to the corresponding web application.

Name

T1003

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

Domain-Name

Value
meethub.gg
aricl.net
airci.net

Url

Value
https://meethub.gg
https://aricl.net
https://airci.net

IPv4-Addr

Value
193.233.132.188
46.101.104.172

External References

- https://www.jamf.com/blog/infostealers-pose-threat-to-macos/
- https://otx.alienvault.com/pulse/660a7b90b7b8567039701a12