Sep 07 2023

NETMANAGEIT

Intelligence Report

Mac users targeted in new malvertising campaign delivering Atomic Stealer

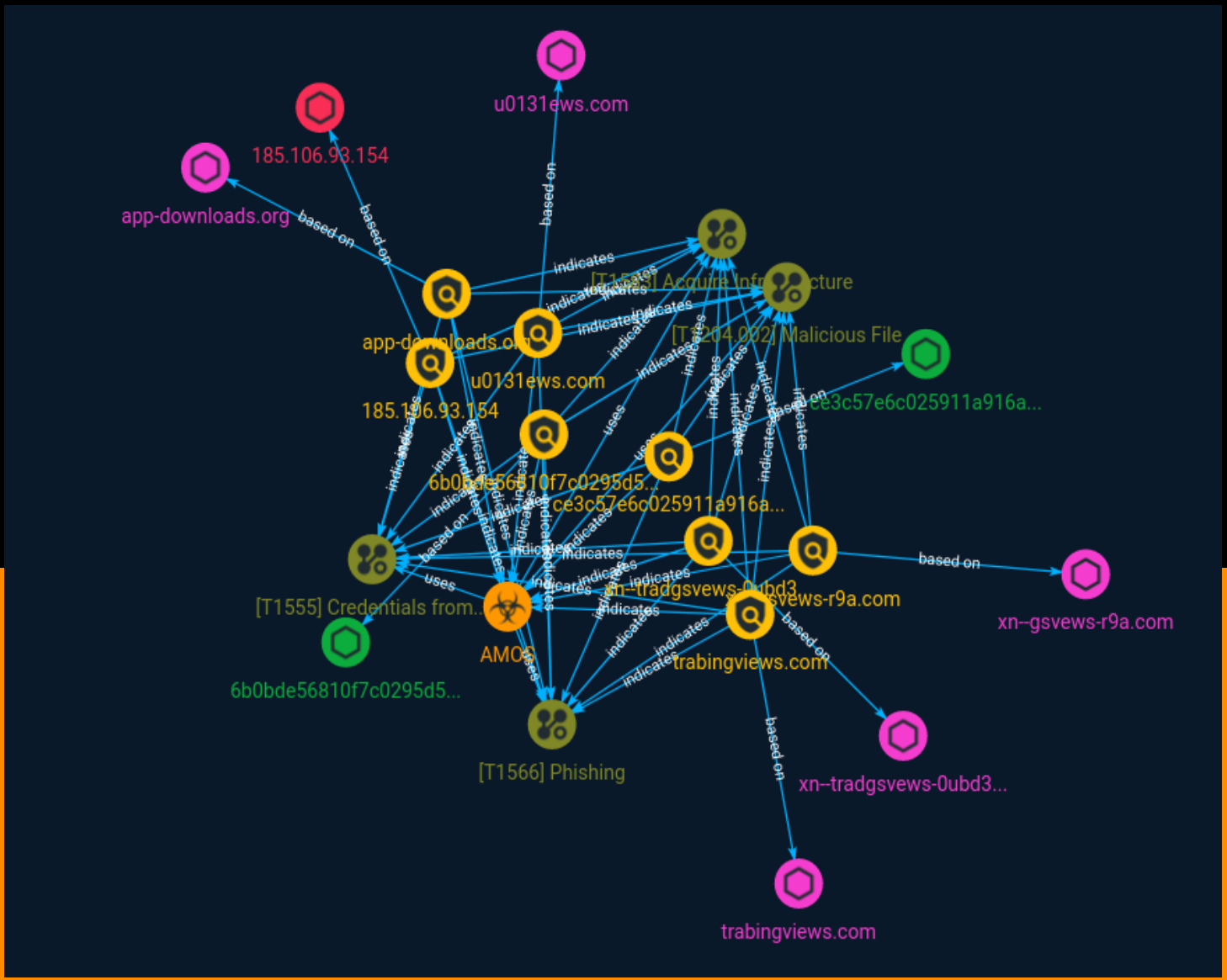

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Malicious ads for Google searches are targeting Mac users. Phishing sites trick victims into downloading what they believe is the app they want. The malware is bundled in an ad-hoc signed app so it cannot be revoked by Apple

Confidence

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

15 / 100

Indicator

Name
u0131ews.com
Pattern Type
stix
Pattern
[domain-name:value = 'u0131ews.com']
Name
xn--tradgsvews-0ubd3y.com
Pattern Type
stix
Pattern
[domain-name:value = 'xn--tradgsvews-0ubd3y.com']
Name
ce3c57e6c025911a916a61a716ff32f2699f3e3a84eb0ebbe892a5d4b8fb9c7a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ce3c57e6c025911a916a61a716ff32f2699f3e3a84eb0ebbe892a5d4b8fb9c7a']

Name

xn--gsvews-r9a.com

Pattern Type

stix

Pattern

[domain-name:value = 'xn--gsvews-r9a.com']

Name

185.106.93.154

Description

ISP: Galaxy LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Thu, 31 Aug 2023 14:46:47 GMT Content-Length: 1018 Content-Type: text/html; charset=utf-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.106.93.154']

Name

trabingviews.com

Pattern Type

stix

Pattern

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

Name

6b0bde56810f7c0295d57c41ffa746544a5370cedbe514e874cf2cd04582f4b0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6b0bde56810f7c0295d57c41ffa746544a5370cedbe514e874cf2cd04582f4b0']

Name

app-downloads.org

Pattern Type

stix
Pattern
[domain-name:value = 'app-downloads.org']

Malware

Name
AMOS

Attack-Pattern

Name
Acquire Infrastructure
ID
T1583
Description
Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090).(Citation: amnesty_nso_pegasus) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.
Name
Phishing
ID
T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Credentials from Password Stores

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 that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name

Malicious File

ID

T1204.002

Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Domain-Name

Value
u0131ews.com
xn--tradgsvews-0ubd3y.com
app-downloads.org
xn--gsvews-r9a.com
trabingviews.com

StixFile

Value
ce3c57e6c025911a916a61a716ff32f2699f3e3a84eb0ebbe892a5d4b8fb9c7a
6b0bde56810f7c0295d57c41ffa746544a5370cedbe514e874cf2cd04582f4b0

IPv4-Addr

Value
185.106.93.154

External References

- https://otx.alienvault.com/pulse/64fa053f6f16dd0914077358
- https://www.malwarebytes.com/blog/threat-intelligence/2023/09/atomic-macos-stealer-delivered-via-malvertising