Mac users targeted in new malvertising campaign delivering Atomic Stealer

malwarebytes.com/blog/threat-intelligence/2023/09/atomic-macos-stealer-delivered-via-malvertising

Jérôme Segura September 6, 2023

Summary

- 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
- The payload is a new version of the recent Atomic Stealer for OSX

Introduction

The majority of the malvertising campaigns we have tracked for the past few months have targeted Windows users. That's not surprising considering that Microsoft holds the largest market share for both desktop and laptop computers.

However, we recently captured a campaign that was pushing both Windows and Mac malware, the latter being an updated version of the new but popular Atomic Stealer (AMOS) for Mac.

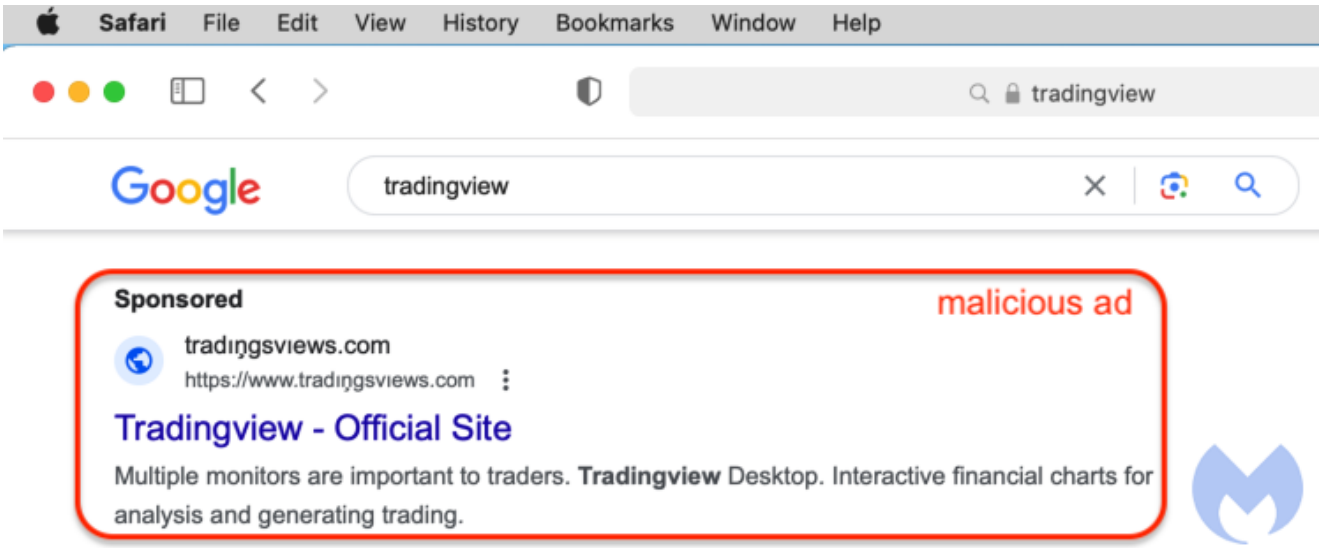
AMOS was first advertised in April 2023 as a stealer for Mac OS with a strong focus on crypto assets, capable of harvesting passwords from browsers and Apple's keychain, as well as featuring a file grabber. The developer has been actively working on the project, releasing a new version at the end of June.

Criminals who buy the toolkit have been distributing it mostly via cracked software downloads but are also impersonating legitimate websites and using ads on search engines such as Google to lure victims in. In this blog post, we will provide details on one campaign targeting TradingView, a popular platform and app to track financial markets.

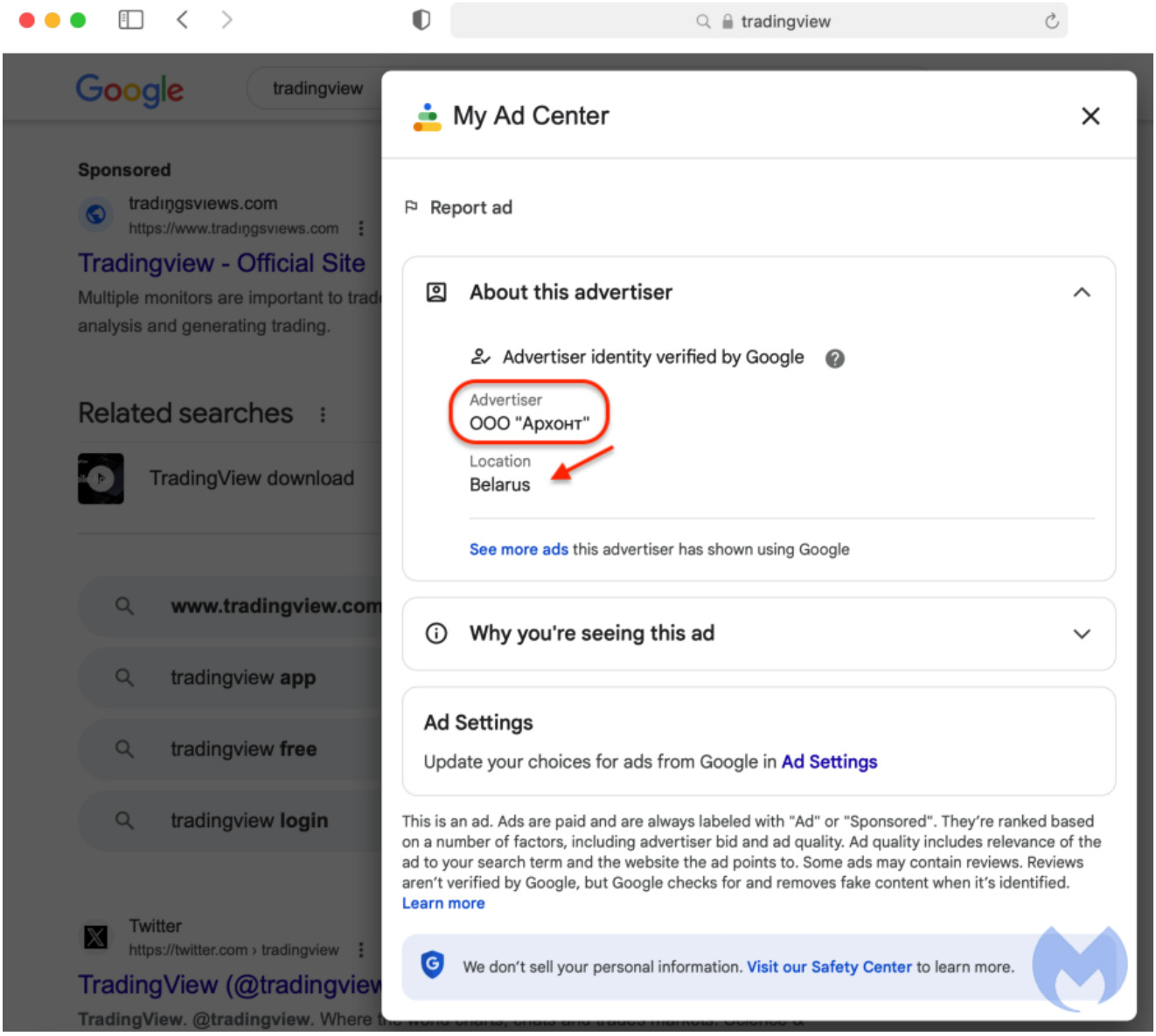
Distribution

Users looking to download a new program will naturally turn to Google and run a search. Threat actors are buying ads matching well-known brands and tricking victims into visiting their site as if it were the official page.

The ad below for TradingView uses special font characters (*tradıŋgsvıews[.]com* is embedded with unicode characters: *trad\u0131\u0146gsv\u0131ews[.]com*) perhaps as an attempt to appear like the real domain and evade detection from Google's ad quality checks:



Google's Ads Transparency Center page shows this advertiser account belongs to someone from Belarus. This is likely a compromised ad account that is being used by the threat actors.

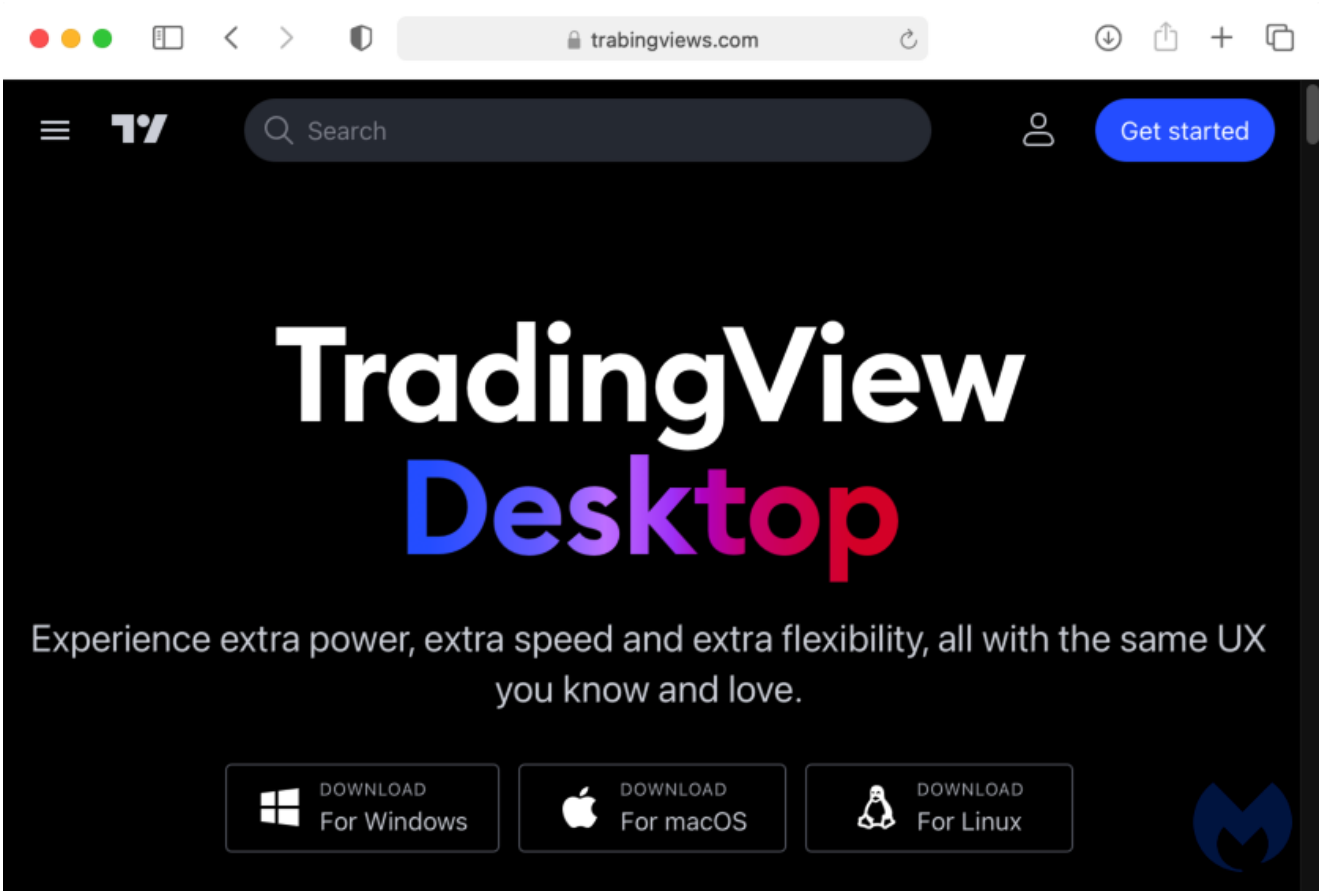


When the user clicks on the ad they are redirected to a phishing page hosted at trabingviews[.]com:

Result	Host	URL	Body
302	www.googleadservices.com	/pagead/aclk?sa=L&ai=DChcSEwjjnauPv4WBAxVtHq0GHa1xBbsYABAAGgJwd...	0
302	xn--tradgsvews-0ubd3y.com	/?utm_source=google&utm_medium=cpc&utm_campaign=g&utm_content=66...	0
302	xn--tradgsvews-0ubd3y.com	/step.html?utm_source=google&utm_medium=cpc&utm_campaign=g&utm_co...	0
200	trabingviews.com	/	97,264

Phishing page

The decoy site (trabingviews[.]com) looks quite authentic and shows three download buttons: one each for Windows, Mac and Linux. One way to detect a potential phishing site is by checking when it was created, which in this case was only a few days ago.



Both the Windows and Linux buttons point to an MSIX installer hosted on Discord that drops NetSupport RAT:

```
https://cdn[.]discordapp[.]com/attachments/1062068770551631992/1146489462025629766/TradingView-x64[.]msix
```

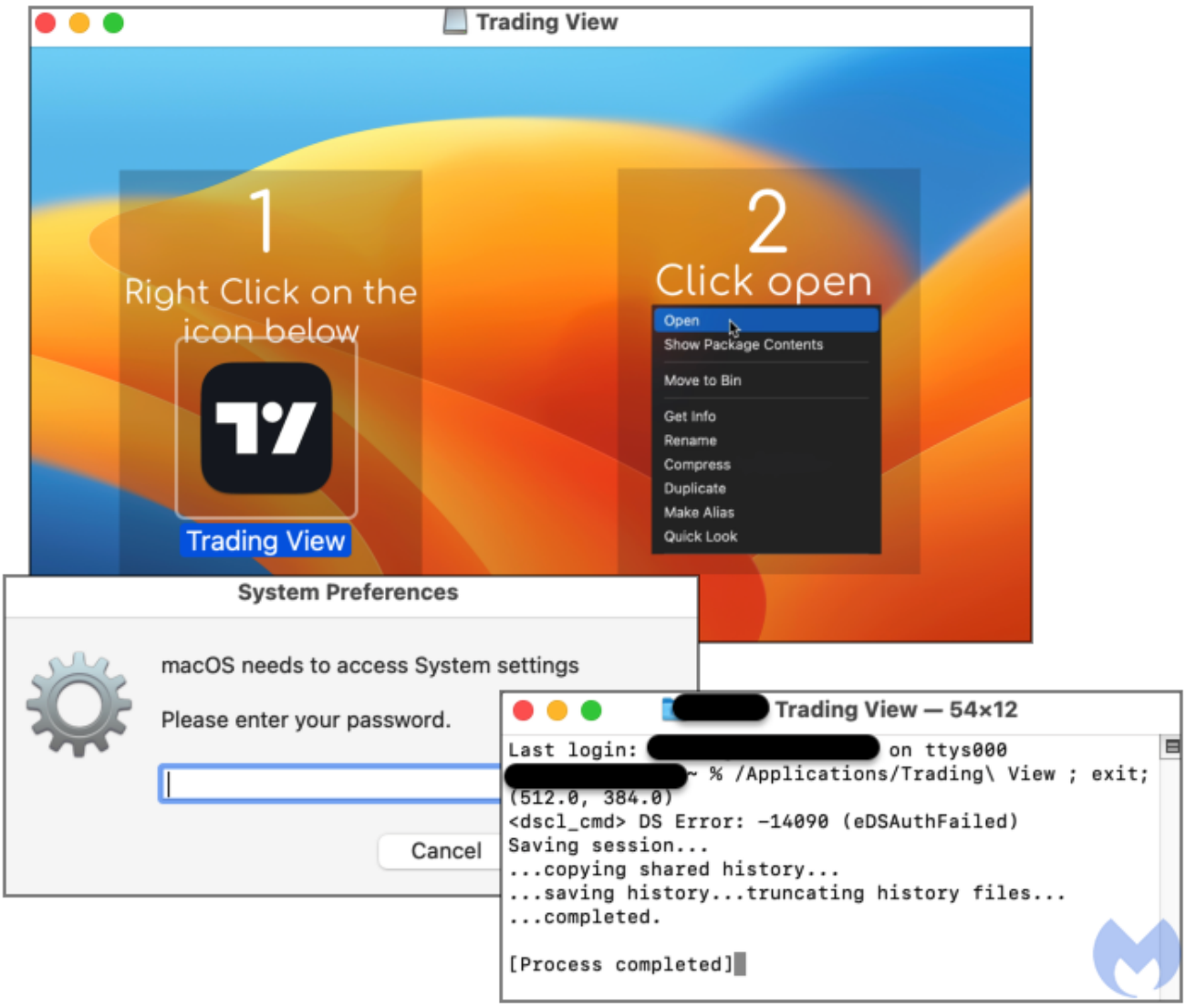
The Mac download is hosted at:

```
https://app-downloads[.]org/tview.php
```

Payload

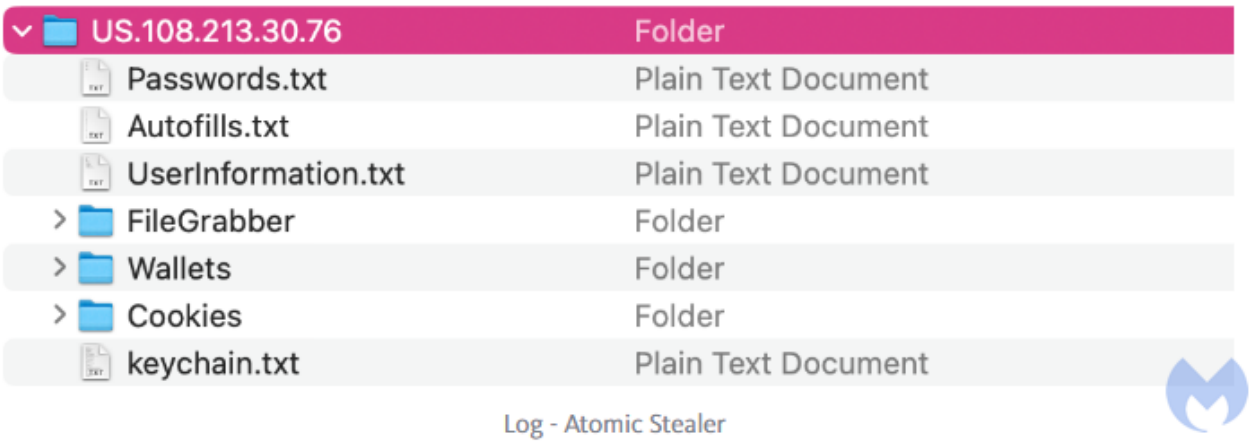
The downloaded file (*TradingView.dmg*) comes with instructions on how to open it in order to bypass GateKeeper. Unlike regular apps, it does not need to be copied into the Mac's Apps folder but is simply mounted and executed.

The malware is bundled in an ad-hoc signed app meaning it's not an Apple certificate, so it cannot be revoked. Once executed, it will keep prompting for the user password in a never ending loop until victims finally relent and type it in.



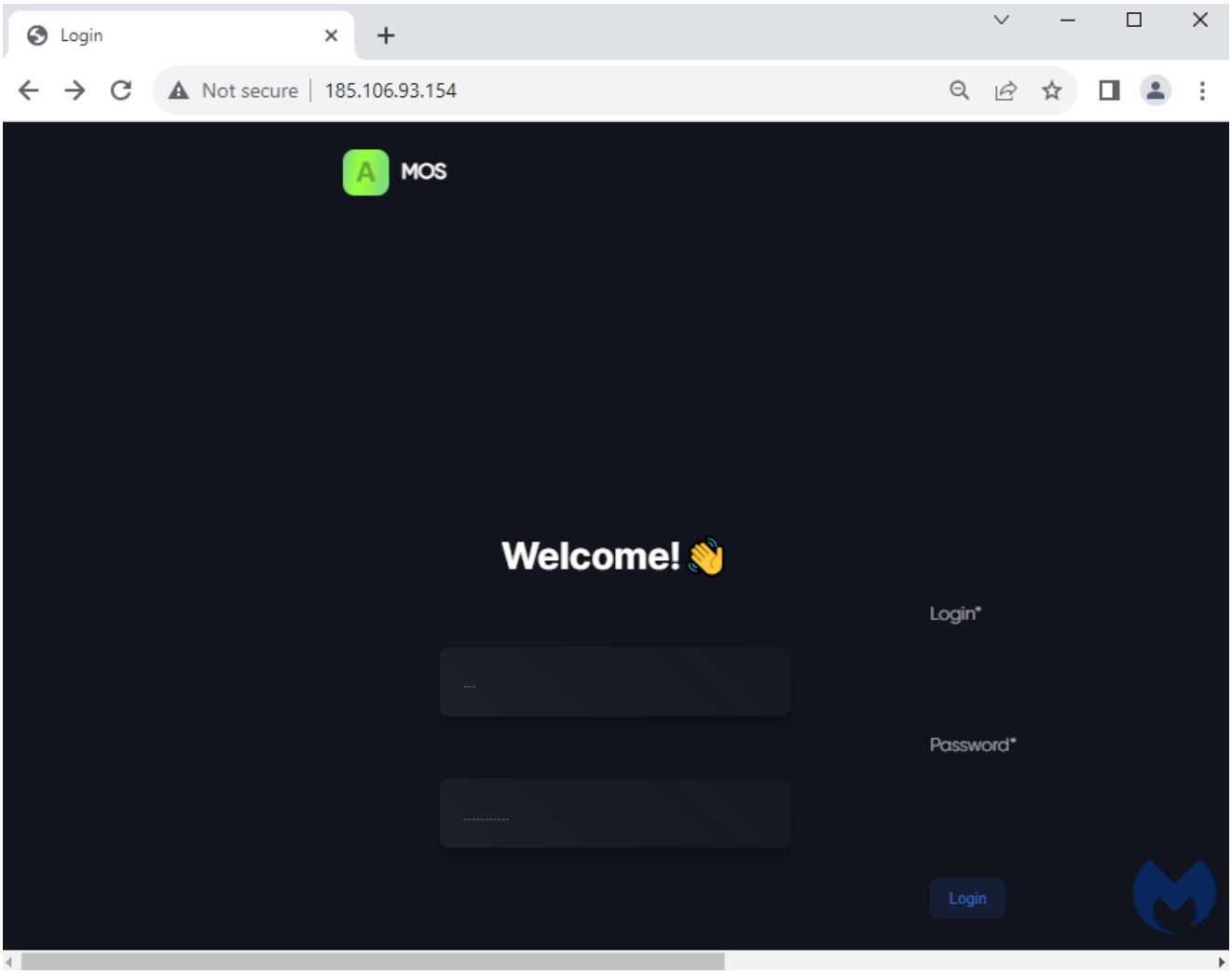
The attacker's goal is to simply run their program and steal data from victims and then immediately exfiltrate it back to their own server. The image below shows the kind of data that can be collected:

General view of the log:



Log - Atomic Stealer

A critical part of any infostealer operation is the back end server that will receive the stolen data. AMOS developers are advising their customers to use a bulletproof server such as the one below:



Protection

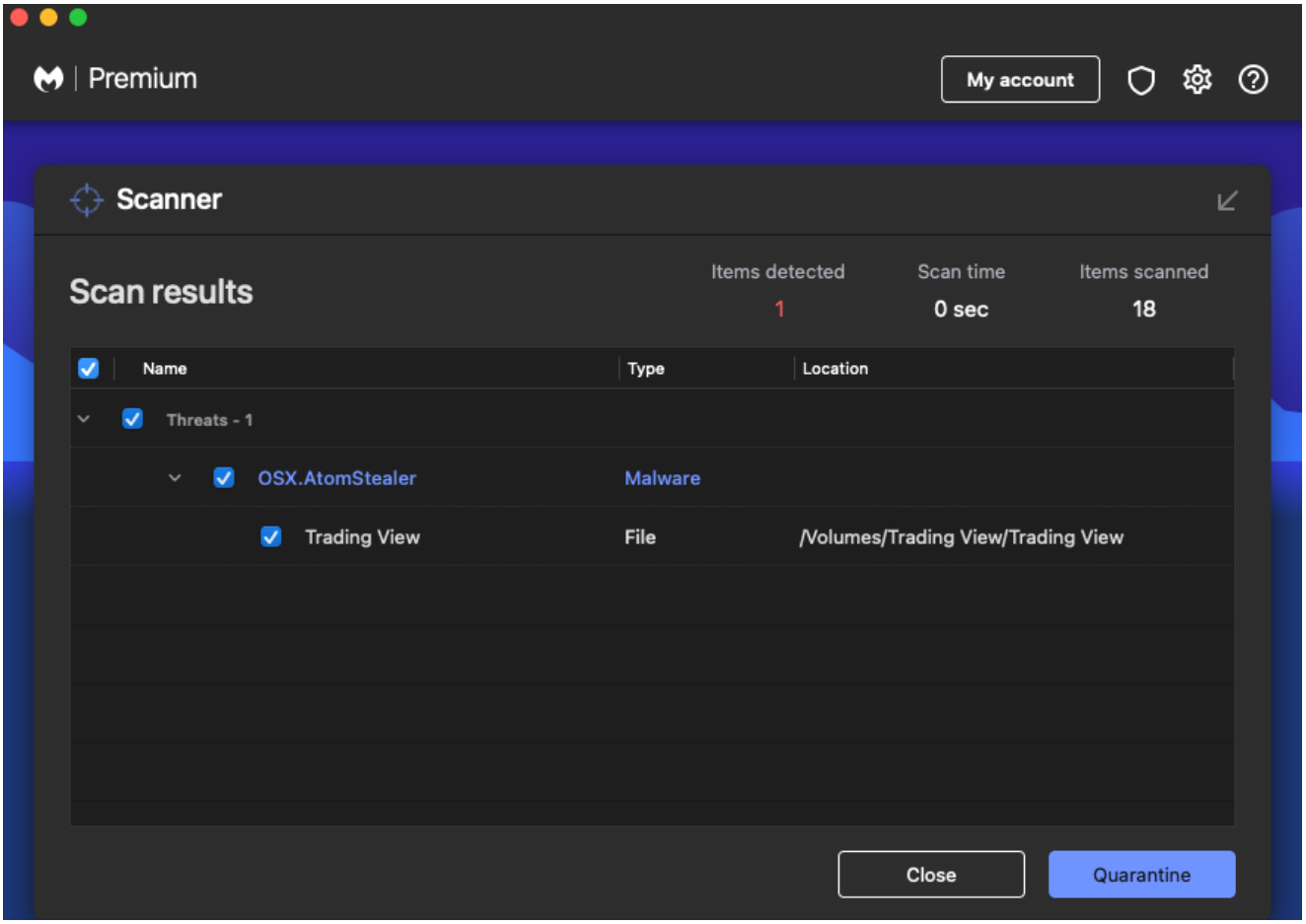
Malvertising continues to be an effective vector to target new victims by abusing the trust they have in their search engines. Malicious ads coupled with professional-looking phishing pages make for a potent combo that can trick just about anyone.

While Mac malware really does exist, it tends to be less detected than its Windows counterpart. The developer or seller for AMOS actually made it a selling point that their toolkit is capable of evading detection.

Before running any new program, make sure to double check its origins. If you clicked on an ad to download a new application, you may want to go back and revisit the official website directly, or at least spend some time verifying that the current website really is the right one, and not a fake.

With stealers such as AMOS, it's also important to run an antivirus that has real time protection so that it blocks the malware before valuable data gets stolen.

Malwarebytes detects this malware as **OSX.AtomStealer**.



Indicators of Compromise

Ad domain:

xn--tradgsvews-0ubd3y[.]com

Phishing domain:

trabingviews[.]com

AMOS installer download:

app-downloads[.]org/tview.php

AMOS installer (dmg):

6b0bde56810f7c0295d57c41ffa746544a5370cedbe514e874cf2cd04582f4b0

AMOS malware:

ce3c57e6c025911a916a61a716ff32f2699f3e3a84eb0ebbe892a5d4b8fb9c7a

AMOS C2:

185.106.93[.]154
