Atomic Stealer rings in the new year with updated version

By Jérôme Segura

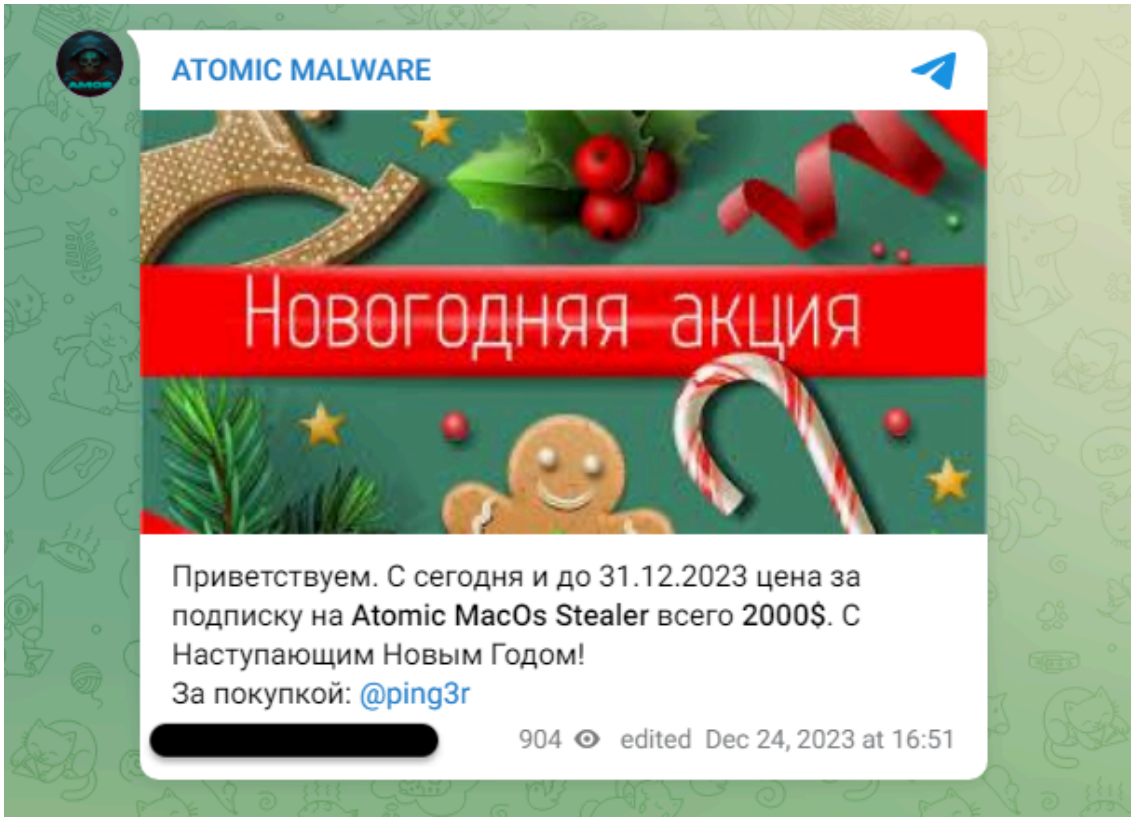
Published: 2024-01-10 · Archived: 2026-04-05 13:38:27 UTC

Last year, we documented malware distribution campaigns both via malvertising and compromised sites delivering Atomic Stealer (AMOS) onto Mac users. This stealer has proven to be quite popular in the criminal underground and its developers have been adding new features to justify its hefty $3000/month rental fee.

It looks like Atomic Stealer was updated around mid to late December 2023, where its developers introduced payload encryption in an effort to bypass detection rules. Some samples from crack websites made their way to VirusTotal around that time frame, followed by a malvertising campaign we observed in January 2024.

In this blog post, we will review the latest changes with Atomic Stealer and the recent distribution with malicious ads via the Google search engine.

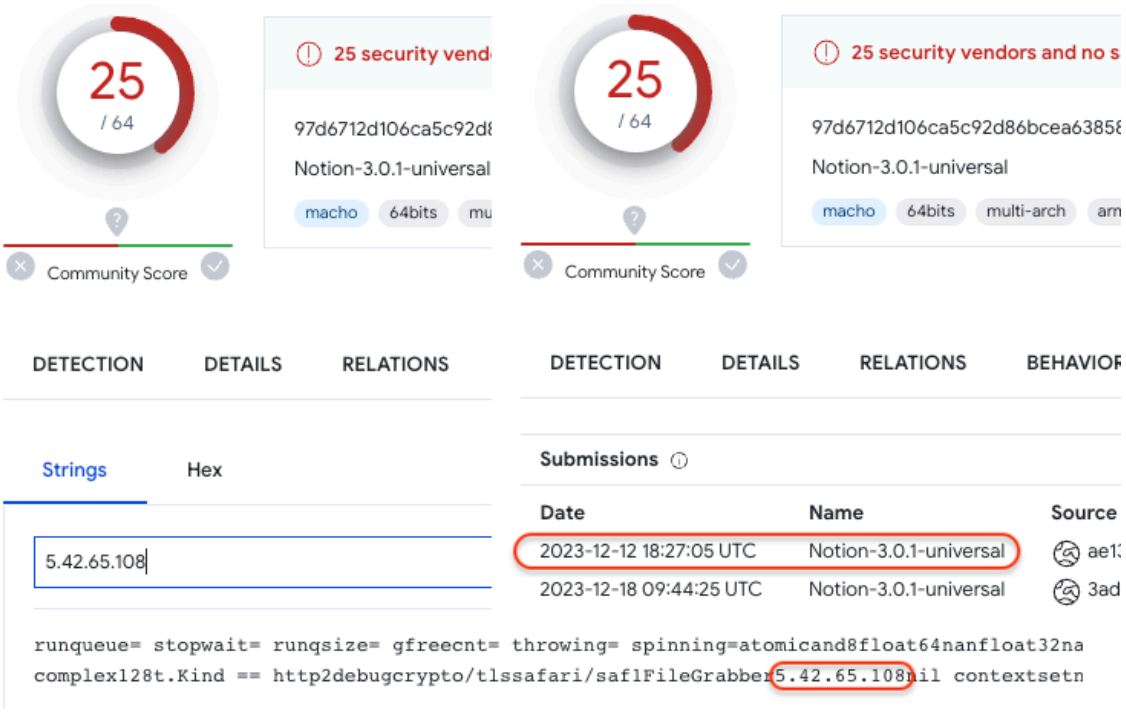
In December, Atomic Stealer ran a promotion via a post on their Telegram channel to offer a special holiday discount to their customers:



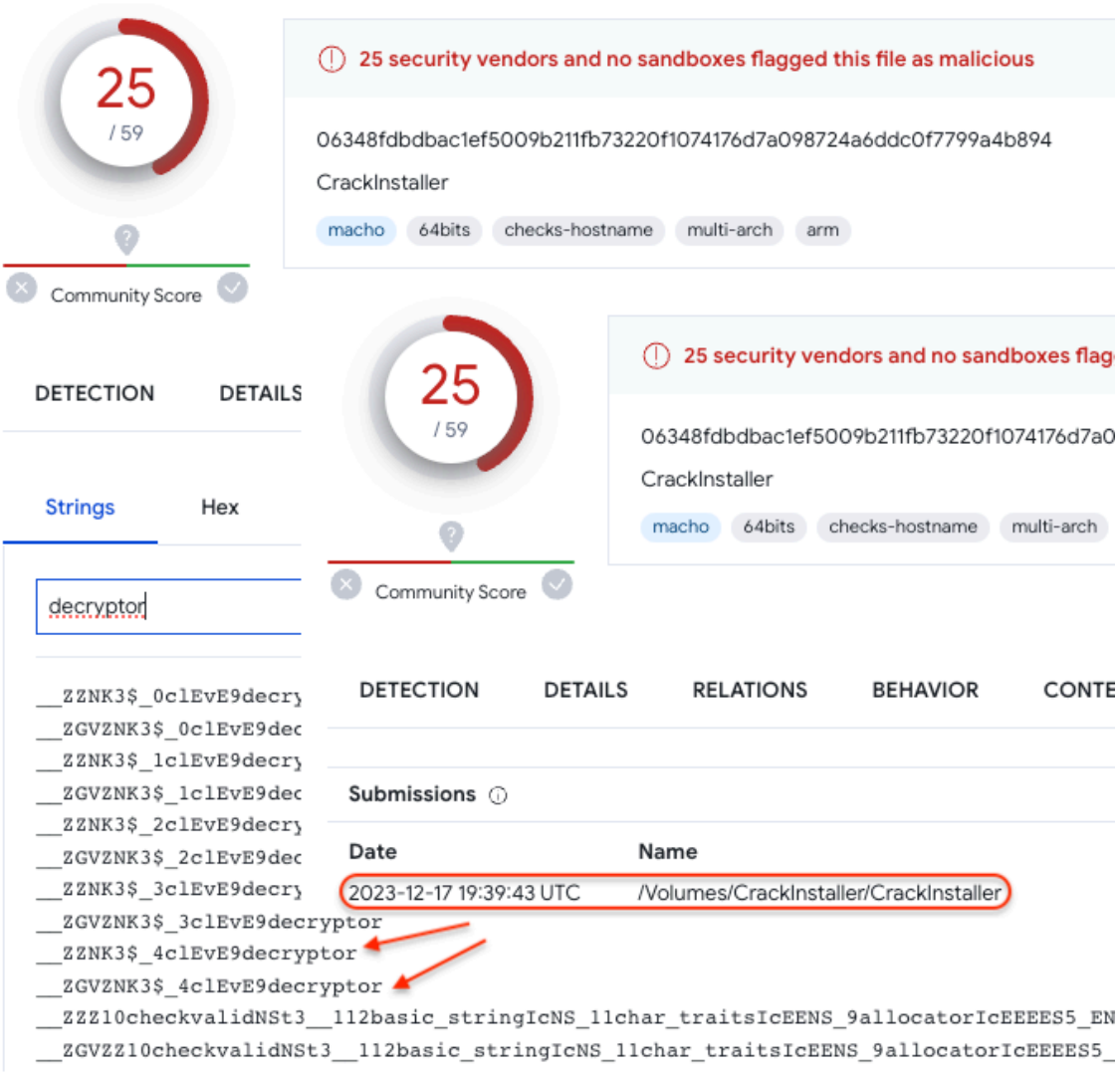
> Welcome. From today until December 31, 2023, the price for a subscription to Atomic MacOs Stealer is only $2000 . Happy New Year!

While the developers did not specifically advertise this feature, it appears that around December 17 Atomic Stealer had changed some of its code to hide certain strings that were previously used for detection and identifying its command and control server.

Sample with strings in clear text (Dec 12), showing for example the IP address for the malware's C2 server:



Obfuscated sample (Dec 17), using a new encryption routine that hides strings of interest:

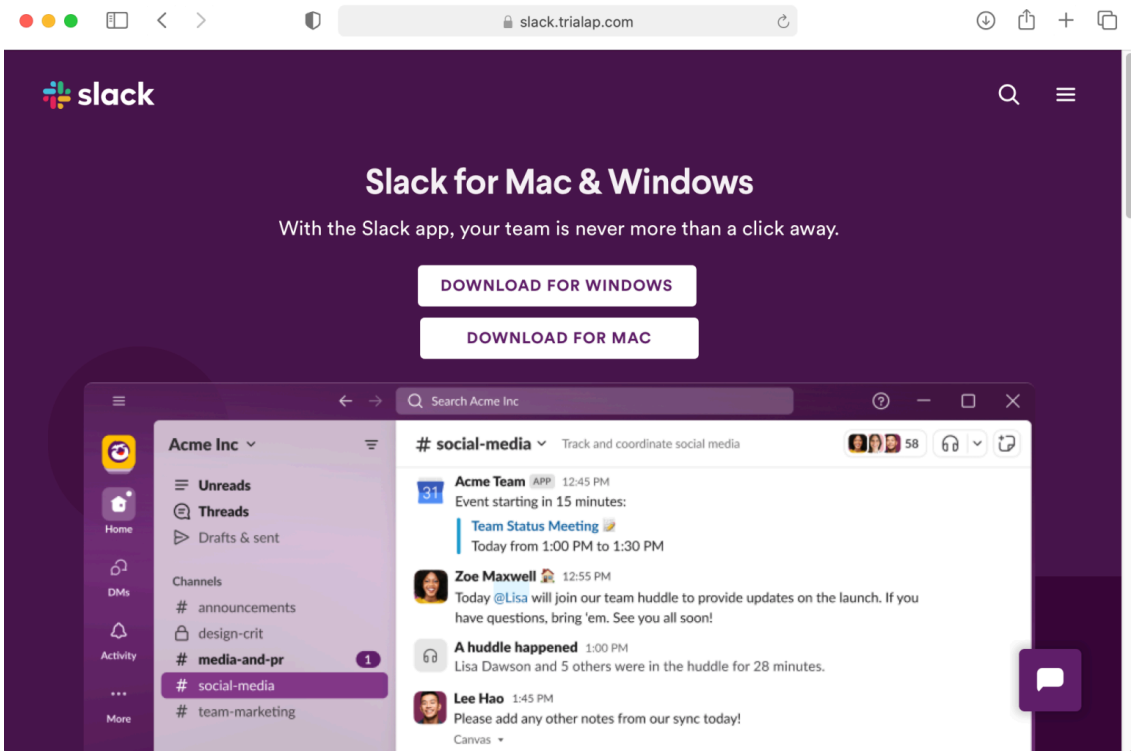


Those two samples above also represent the different distribution channels that Atomic Stealer customers are using to distribute the malware. It's possible customers using software cracks got access to the update Atomic Stealer before those that leverage malicious ads.

In fact, during the holiday break, we noticed a decrease in malvertising activity, in particular for the campaigns running via Google search ads. This was somewhat expected and typically extends into early January. However, on January 8, we identified a malvertising campaign using similar tactics seen previously by threat actors distributing FakeBat. In this instance, there was also a payload destined for Mac users, Atomic Stealer in its updated version.

Malvertising with FakeBat – Atomic Stealer combo

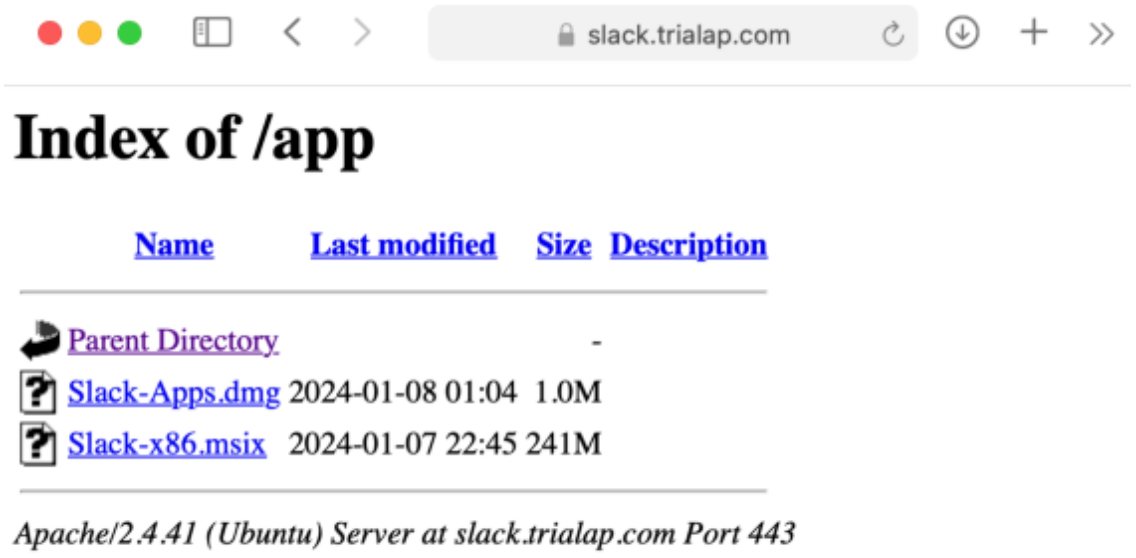
The threat actors are luring victims via a Google search ad impersonating Slack, the popular communication tool, and redirecting them to a decoy website where the app can be downloaded for both Windows and Mac:



The threat actors are leveraging tracking templates to filter traffic and route it through a few redirects before loading the landing page:

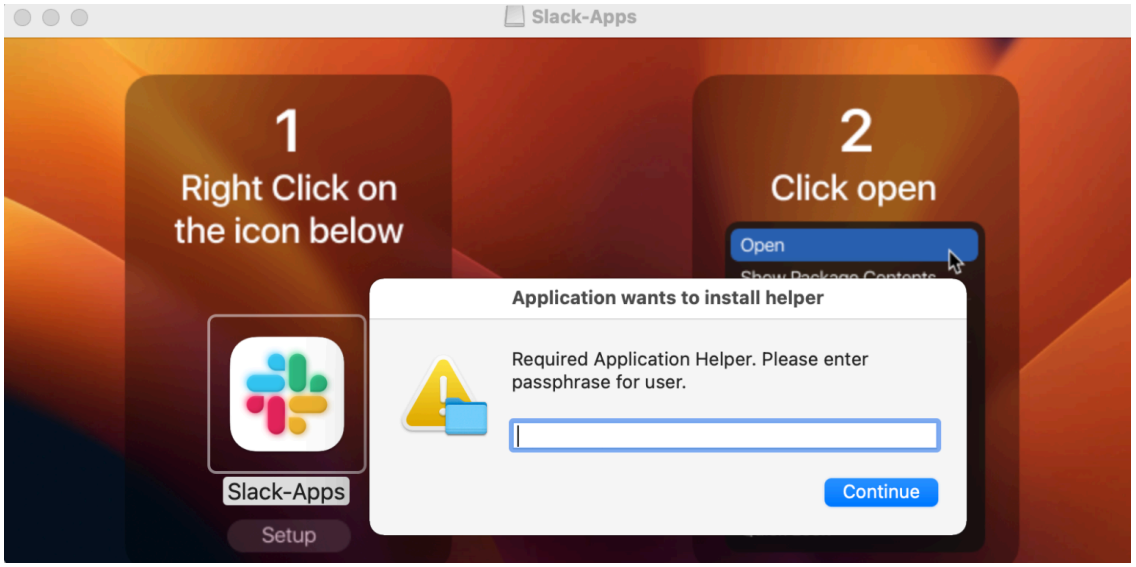
Host	URL
www.googleadservices.com	/pagead/aclk?sa=L&ai=DChcSEwi5vKi46M6DAxUTDa0GHYAsA...
ivchlo.gotrackier.com	/click?campaign_id=2&pub_id=2&force_transparent=true&url...
ivchlo.gotrackier.com	/click?campaign_id=1&pub_id=2&
red.seecho.net	/
red.seecho.net	/
slack.trialap.com	/

On that same domain, there is an open directory showing the location of the Windows payload which is an MSI installer (FakeBat), and the Mac one, Atomic Stealer (AMOS):



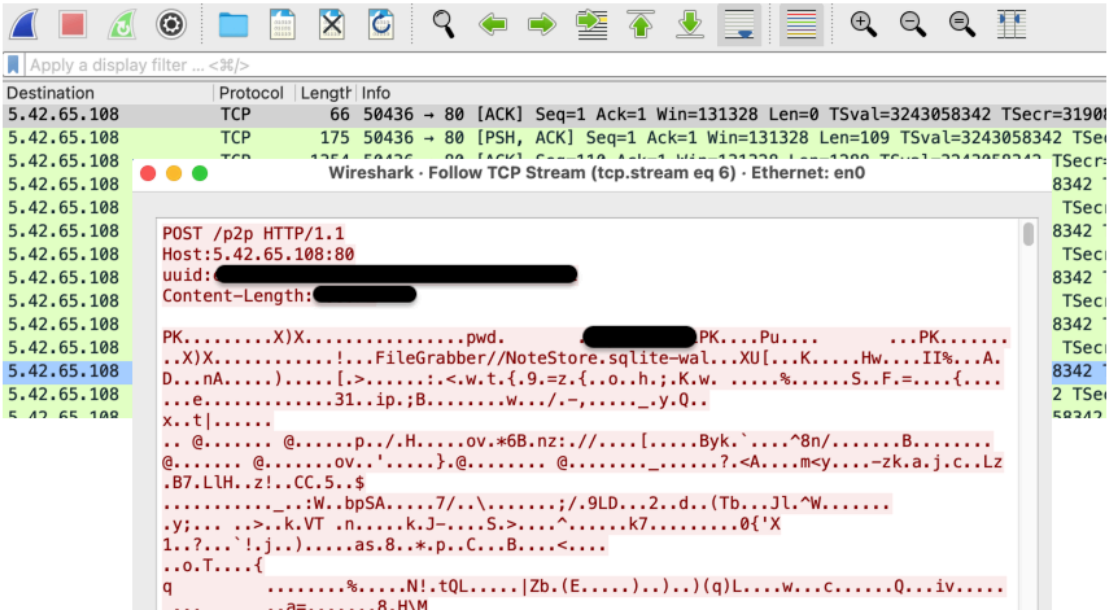
Obfuscated Atomic Stealer

The malicious DMG file contains instructions for users to open the file as well as a dialog window asking them to enter their system password. This will allow Atomic Stealer to collect passwords and other sensitive files that are typically access-restricted.



When comparing the previous Atomic Stealer samples we have, we can see that the application code has changed. Previously, we could see certain strings revealing the nature of the payload (browsers, wallets, etc.) and more importantly the command and control server that receives stolen user data. Now, these strings are no longer visible as the code is well obfuscated:

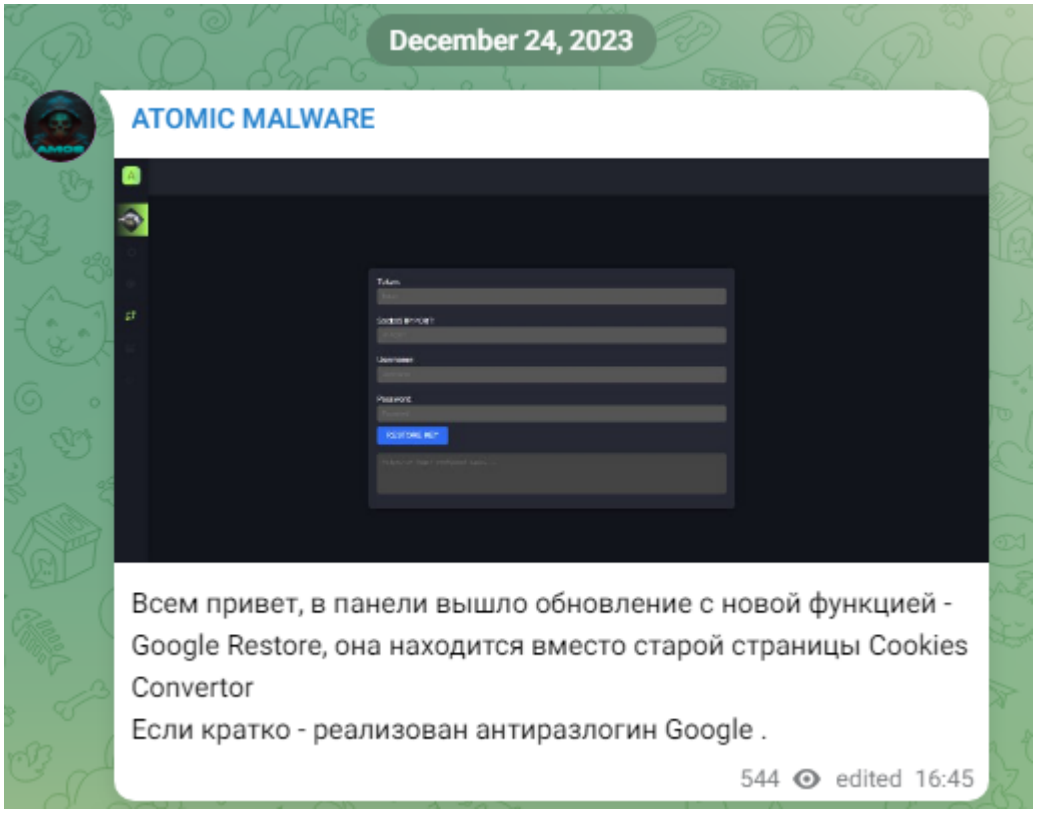
When we analyzed this sample in a sandbox we saw the data exfiltration taking place and the corresponding C2 server:



Stealing victim passwords, crypto wallets and cookies

As detailed in Objective-See's The Mac Malware of 2023, stealers were the most popular type of malware. It's not just passwords that are of interest to cyber criminals. Stealing browser cookies can sometimes be even better than having the victim's password, enabling authentication into accounts via session tokens.

In fact, Atomic Stealer developers were working on a cookie feature they announced on Christmas Eve:

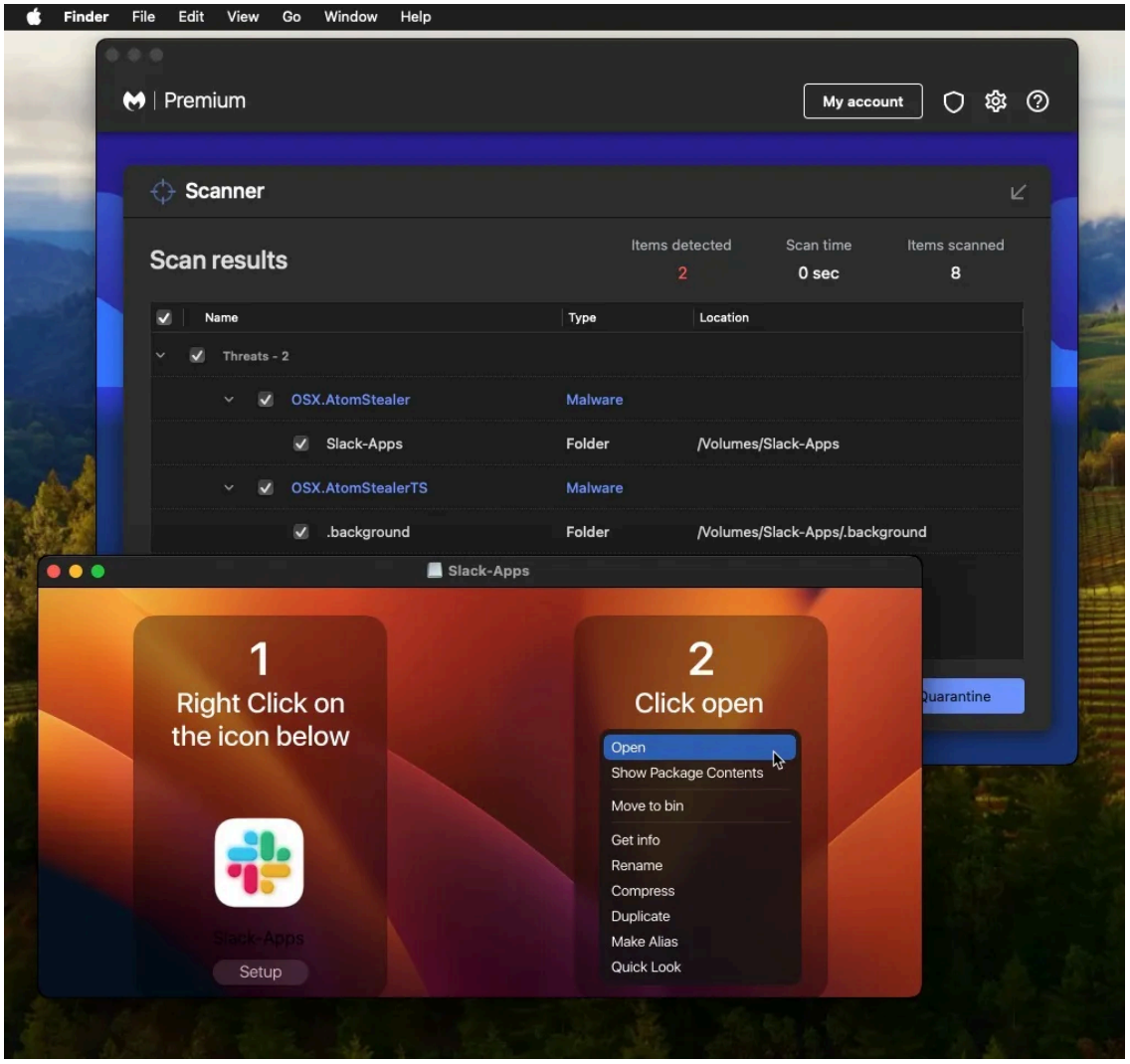


> Hi everyone, the panel has released an update with a new feature – Google Restore, it is located instead of the old page Cookies Convertor. In brief – implemented anti-unlogin Google.

As stealers continue to be a top threat for Mac users, it is important to download software from trusted locations. Malicious ads and decoy sites can be very misleading though and it only takes a single mistake (entering your password) for the malware to collect and exfiltrate your data.

We have reported the malicious ad and infrastructure to the respective parties for mitigation.

To stay safe from this and other similar threats, a combination of web protection and antivirus is best suited. Malwarebytes Browser Guard and Antivirus for macOS can prevent and detect Atomic Stealer.



Indicators of Compromise

Malvertising chain

```
ivchlo[.]gotrackier[.]com
red[.]seecho[.]net
```

Decoy site

```
slack[.]trialap[.]com
```

FakeBat payload URL

```
slack[.]trialap[.]com/app/Slack-x86.msix
```

FakeBat hash

```
49f12d913ad19d4608c1596cf24e7b6fff14975418f09e2c1ad37f231943fda3
```

FakeBat C2

```
ads-strong[.]online
```

Atomic Stealer payload URL

```
slack[.]trialap[.]com/app/Slack-Apps.dmg
```

Atomic Stealer hash

```
18bc97e3f68864845c719754d2d667bb03f754f6e87428e33f9c763a8e6a704a
```

C2

```
5.42.65[.]108
```
