Atomic Stealer for macOS has been updated

Ray Fernandez

Atomic Stealer (AMOS), a piece of malware popular among cybercriminals that target Mac devices, has been updated, making it more difficult to detect.

As Moonlock reported in November 2023, AMOS was tricking Mac users by posing as a fake browser update. Now, researchers have discovered that AMOS hackers are using Google Ads and impersonating the popular messaging app Slack to target new victims. Let's look into the new AMOS modifications, what AMOS can do, and how you can stay safe.

The updated 2024 Atomic Stealer

Malwarebytes reported on January 10 that AMOS was updated in late December 2023. The new additions to the malware, sold in the cybercriminal world for a costly $3,000/month rental fee, include payload encryption and a feature called Google Restore.

Google Restore: New Google “anti-unlogin” cookie password stealer

Moonlock recently reported that cybercriminal groups have been integrating a new exploit into their malware-as-a-service products. This new exploit is capable of regenerating the victim’s browser cookies and tokens. This allows hackers to steal credentials even if the user changes the password.

One of the new AMOS updates, known as Google Restore, seems to align with this type of new exploit. The AMOS group described the new integrated feature in a post on their Telegram channel in December. “In brief,” said AMOS, “(we) implemented anti-unlogin Google.”

Another new AMOS feature: Payload encryption

On the other hand, the other new feature that AMOS built into its malware stealer is payload encryption. In this case, AMOS bad actors use payload encryption to bypass detection rules and fly comfortably under the radar.

By encrypting the payload — encoding the data during the transmission of exfiltrated data — AMOS malware makes strings unreadable.

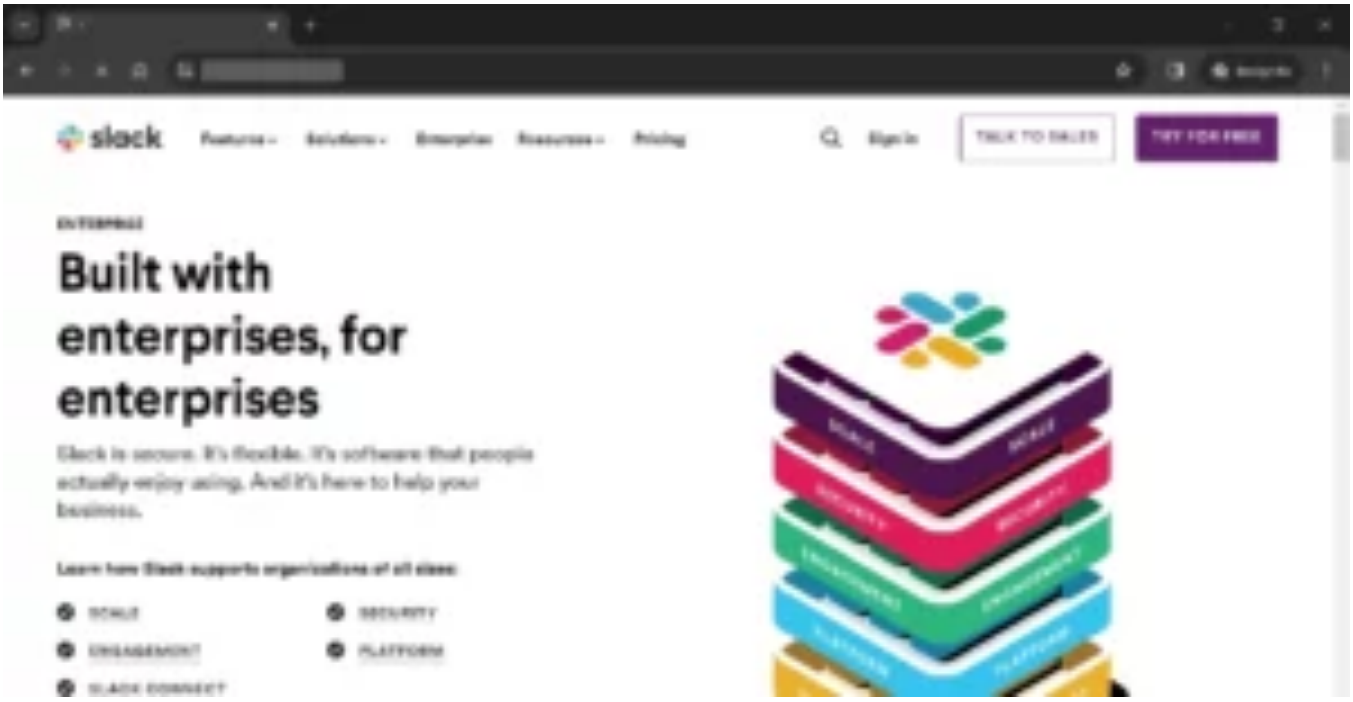
Malwarebytes compared the previous Atomic Stealer samples with the new AMOS updated malware and concluded that the application code had changed. For experts who knew where to look, the previous version of the malware revealed important data about the malware’s transmissions. This data included details on browsers, wallets, and other assets, as well as data from the AMOS command and control server that receives the stolen user data.

“Now, these strings are no longer visible, as the code is well obfuscated,” Malwarebytes’ Jérôme Segura wrote in the recent AMOS research blog.

Targeting users with fake Google Ads and Slack impersonation

Another new move for AMOS hackers is the use of fake websites that are almost identical to Slack download pages. Using Google Ads, AMOS redirects users to malware chain sites such as ivchlo[.]gotrackier[.]com, or red[.]seecho[.]net. These, in turn, redirect users to the decoy sites like slack[.]trialap[.]com.

When potential victims are redirected to these fake sites and click Download, a malicious DMG file kicks in. The DMG file poses as a legitimate Slack download package and attempts to convince users to install the malware with a well-designed step-by-step instruction-to-install user interface that takes over the screen.



ENTERPRISE

Built with enterprises, for enterprises

Slack is secure. It's flexible. It's software that people actually enjoy using. And it's here to help your business.

Learn how Slack supports organizations of all sizes:

- SCALE
- SECURITY
- ENGAGEMENT
- PLATFORM
- SLACK CONNECT

A screenshot of the AMOS Atomic Stealer posing as a Slack download page.

Once AMOS is installed, it automatically starts to steal sensitive data and passwords as well as access-restricted files. Atomic Stealer can steal keychain passwords, user documents, cookies, browser data, credit card details, cryptocurrency wallets, and much more. This malware, now posing as Slack, can target both Mac and Windows users, delivering different malware files depending on what system the victim is running.

How can I keep my Mac safe from Atomic Stealer?

Stealers are expected to continue targeting Mac and Apple devices throughout 2024 as this type of malware rises in popularity on the cybercriminal market. Bad actors will continue to update these ready-to-use stealers, giving them better evasion, breach, persistent, and exfiltration features and capabilities. Faced with these inevitable criminal trends, users need to step up their game to keep safe.

Staying up to date with news on stealers like AMOS is crucial. And while these stealers may be state-of-the-art, they still rely heavily on user error to breach a system. This means that users must click on links, download files, and respond to messages for damage to be done.

As a rule of thumb, always think twice before downloading an app, a program, or a file. Additionally, pay close attention to the HTML address of a website and double-check if it is legitimate. Google Ads and other online ad platforms are used by cybercriminals as bait tools because most users assume that bypassing Google Ads' strong security policy is impossible. Evidently, criminals can promote malicious sites on these platforms, so try not to click on ads.

It is also important to understand that bad actors are masters of impersonation and social engineering techniques. They excel at misleading victims. As Malwarebytes writes, “It only takes a single mistake (entering your password) for the malware to collect and exfiltrate your data.”

To build up your security posture, set your browser to the highest privacy and security settings. Use strong passwords and multi-factor authentication (biometrics if possible). And download and use trusted and professional antimalware. Antimalware technology can detect if any malware or malicious actions attempt to breach your system. It will warn you of the attack and shut it down before it even starts.

Finally, also stay tuned for more 2024 AMOS news. It is highly unlikely that this is the last time we will hear from this Mac stealer.

This is an independent publication, and it has not been authorized, sponsored, or otherwise approved by Google LLC. Google Ads is a trademark of Google LLC.

Ray has been covering tech and cybersecurity for over 15 years. His work has appeared on TechRepublic, VentureBeat, Forbes, Entrepreneur, and the Microsoft Blog, among others.

You might also like

Jan 11, 2024

3 min read

Dec 21, 2023

5 min read

Dec 15, 2023

5 min read