New ‘Atomic macOS Stealer’ Malware Offered for $1,000 Per Month

A new piece of macOS malware named ‘Atomic macOS Stealer’, or AMOS, appears to provide a wide range of data theft capabilities, targeting passwords, files, and other types of information.

Researchers at threat intelligence firm Cyble have analyzed a sample of the AMOS malware that was uploaded recently to VirusTotal and which had zero detections on the malware analysis platform at the time of its discovery – at the time of writing it is detected by one antimalware engine.

According to Cyble, the malware, advertised on a Telegram channel, has been offered for $1,000 per month. Its author claims it can steal all passwords from the Keychain, full system information, and files from the compromised computer.

It can also allegedly steal passwords, cookies, cryptocurrency wallets and payment card data from browsers such as Chrome, Firefox, Brave, Edge, Vivaldi, Yandex and Opera. In addition, it can steal cryptocurrency wallets outside the web browser and from browser extensions.

Users of the malware are provided a web-based management interface hosted on a .ru domain, and exfiltrated data can also be sent to specified Telegram channels.

The malware is delivered as a .dmg file and, when first executed, it displays a fake prompt to trick the victim into handing over their macOS system password.

A researcher from Trellix has also analyzed the malware and noticed that an IP address used by AMOS might be linked to Raccoon Stealer, a piece of malware previously tied to Russian and Ukrainian threat actors.

It’s unclear if the malware is signed and how much effort it takes to get it to bypass macOS security features and get it to execute on a system. In many cases, malware designed to run on macOS may appear to have numerous capabilities, but actually getting it to execute on targeted systems is not an easy task.

Related: North Korean Hackers Use Fake Job Offers to Deliver New macOS Malware

Related: Chinese Cyberspies Use Supply Chain Attack to Deliver

Windows, macOS Malware

Related: New macOS Malware ‘DazzleSpy’ Used in Hong Kong Attacks

> *New ‘Atomic macOS Stealer’ Malware Offered for $1,000 Per Month*