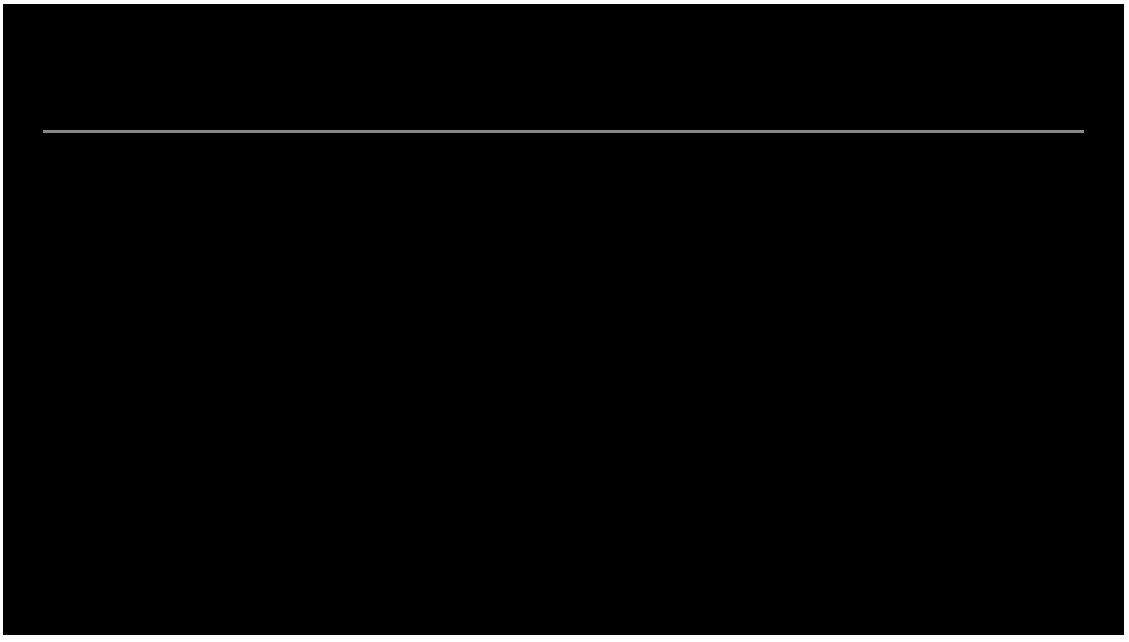
Apple picking: Bobbing for Atomic Stealer & other macOS malware

By susannah.matt@redcanary.com

Published: 2024-10-10 · Archived: 2026-04-06 01:29:00 UTC

For years, macOS has enjoyed a reputation as being relatively secure from widespread malware threats compared to its Windows counterpart. The occasional ad fraud, remote access malware, or ransomware incident would surface, but nothing that seemed like an existential threat to enterprises. In fact, many people still hold the belief that macOS is immune to malware—a dangerous misconception.

However, 2024 has shattered that illusion. A surge in macOS-focused malware, including notorious threats like Atomic Stealer, Poseidon Stealer, and Cthulhu Stealer, has marked a significant shift. Adversaries are increasingly targeting macOS devices, recognizing their growing presence in enterprises and the critical data contained within.



macOS as a new target

As macOS systems become more ingrained in corporate environments—used not just by developers, but by teams across sales, marketing, and engineering—they've become prime targets for cybercriminals. These systems often house valuable organizational secrets, credentials, and even deployment keys used by software developers, making them a treasure trove for adversaries.

Atomic Stealer enters the chat

Atomic Stealer has caught our attention as an outlier in our 2024 midyear update since it's a macOS malware family making its presence known amidst a stockpile of threats targeting Windows. It's a sophisticated, all-in-one

tool that allows adversaries to vacuum up a wide array of sensitive information, from browser cookies and credentials to access tokens. Once deployed, Atomic Stealer can harvest hundreds, if not thousands, of data points from a single machine—data that can be sold on the black market or leveraged for further attacks.

The following shows the rough timeline of an Atomic Stealer infection:

Detection opportunities

Fortunately, Atomic Stealer is very detectable, and so we're going to share a pair of pseudo-detectors that pretty reliably catch the malware's credential access behaviors. Note that these detection opportunities may require tuning within your environment—and they may also catch other macOS threats.

Abusing OSX shell to gather passwords

process == [`sh`]

&&

command_line_includes (`system preferences` || `password`)

Abusing AppleScript to gather passwords

process_name == `osascript`

&&

command_line_includes (`display dialog` && `password`)

Why enterprise businesses should be concerned

The rising popularity of macOS in the enterprise means that organizations can no longer afford to treat Mac security as an afterthought. With adversaries specifically designing malware to exploit macOS vulnerabilities, it's clear that these devices are no longer just niche tools for creative professionals or developers. They are deeply embedded in the workflows of many modern companies, and as such, they need robust protection.

> Organizations can no longer afford to treat Mac security as an afterthought.

Organizations that have a large macOS footprint—those who are primarily or exclusively Mac-based—typically have a better understanding of the risks. But if you're in a Windows-native environment with just a handful of Macs, it's easy to overlook these systems as less critical. That mindset, however, leaves a dangerous gap in your security posture.

How to secure macOS devices

The first step in defending macOS systems is understanding your Mac footprint. How many macOS devices are in your environment? What are they used for? Once you have a clear picture, it's time to implement strong security measures.

Just like Windows systems, macOS devices should have comprehensive protections in place, including:

- antivirus
- anti-malware controls
- endpoint detection and response (EDR)

Investigating macOS malware can be particularly challenging for defenders who have spent their careers working on Windows systems. However, with the right tools—like EDR solutions tailored for macOS—security teams can more effectively detect and mitigate threats like Atomic Stealer without unnecessary hassle. For those investigating macOS stealers in malware analysis, consider checking out Red Canary Mac Monitor to help gather data.

The rise of macOS-specific malware like Atomic Stealer highlights the need for organizations to reassess their approach to Mac security. As macOS becomes a staple in the enterprise, adversaries are more determined than ever to exploit these systems for profit. By understanding your macOS footprint and implementing robust prevention and detection measures, you can keep your valuable data out of the hands of cybercriminals.
