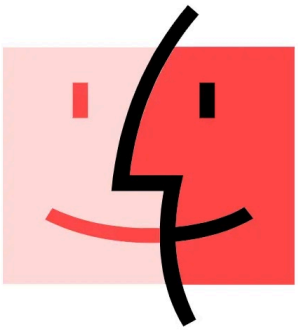
Password Stealing Malware Attacking macOS Users Increasing Rapidly

By **Tushar Subhra Dutta** - February 6, 2025



In recent months, macOS users have faced a significant rise in password-stealing malware attacks.

These threats, often distributed through malicious advertising and fake application installers, have become increasingly sophisticated.

Three prominent malware types, “Atomic Stealer,” “Poseidon Stealer,” and “Cthulhu Stealer” are at the forefront of this surge.

While the security analysts at Palo Alto Networks’ Unit42 noted that each of the stealer comes with unique methods of operation and distribution.

Stealer Analysis

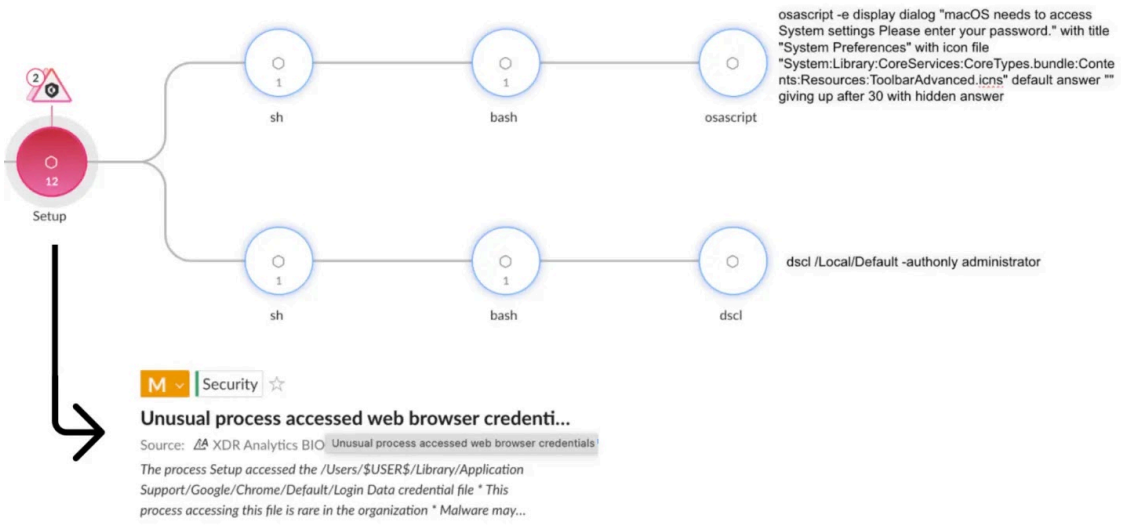
Atomic Stealer: Atomic Stealer, also known as AMOS, was first discovered in April 2023. It is sold as a malware-as-a-service (MaaS) on hacker forums and Telegram.

The malware has evolved through several versions, initially written in Go and later in C++. Some versions include Python scripts or Mach-O binaries.

Atomic Stealer is primarily distributed via malvertising and targets sensitive data such as browser passwords, cryptocurrency wallets, and instant messaging data.

Execution Flow of Atomic Stealer:-

Atomic Stealer disguises itself as a legitimate installation file. It attempts to access files like `/Users/$USER/Library/Application Support/Google/Chrome/Default/Login Data`, which stores Google Chrome login credentials.

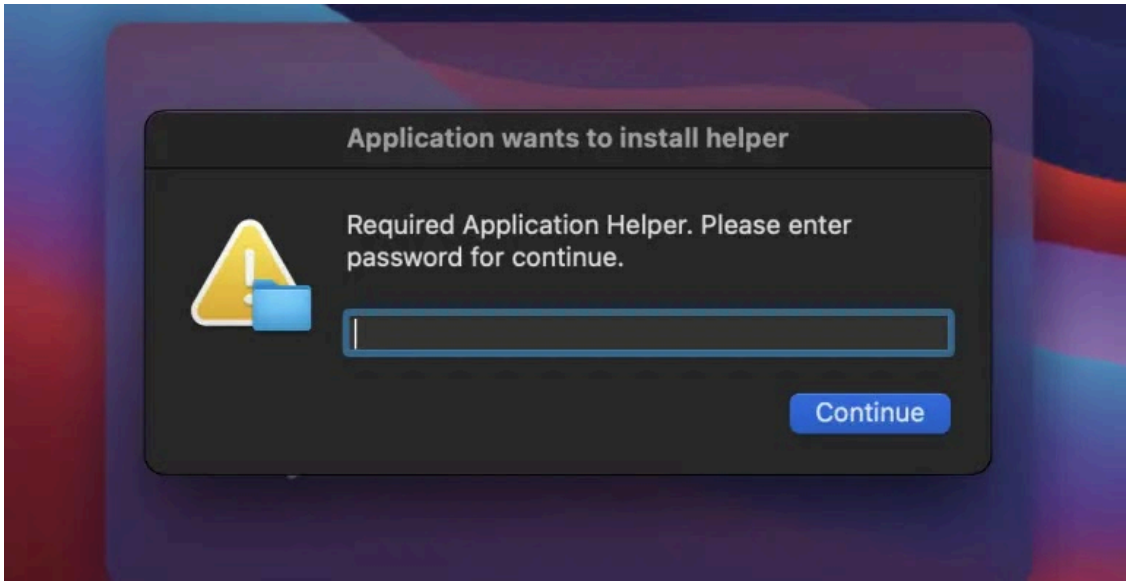


Execution of Atomic Stealer (Source – Palo Alto Networks)

Poseidon Stealer: Poseidon Stealer is advertised by "Rodrigo4," allegedly a former Atomic Stealer developer. It is distributed via Trojanized installers that mimic legitimate applications, often through Google ads and malicious emails. The malware uses an encoded AppleScript to execute its main logic, prompting victims for passwords during installation.

Poseidon Stealer's Operation:-

After installation, Poseidon Stealer prompts users with a dialog box to obtain their password. It steals browser passwords, cryptocurrency wallets, notes from macOS Notes, and Telegram data, sending this information to attacker-controlled servers.



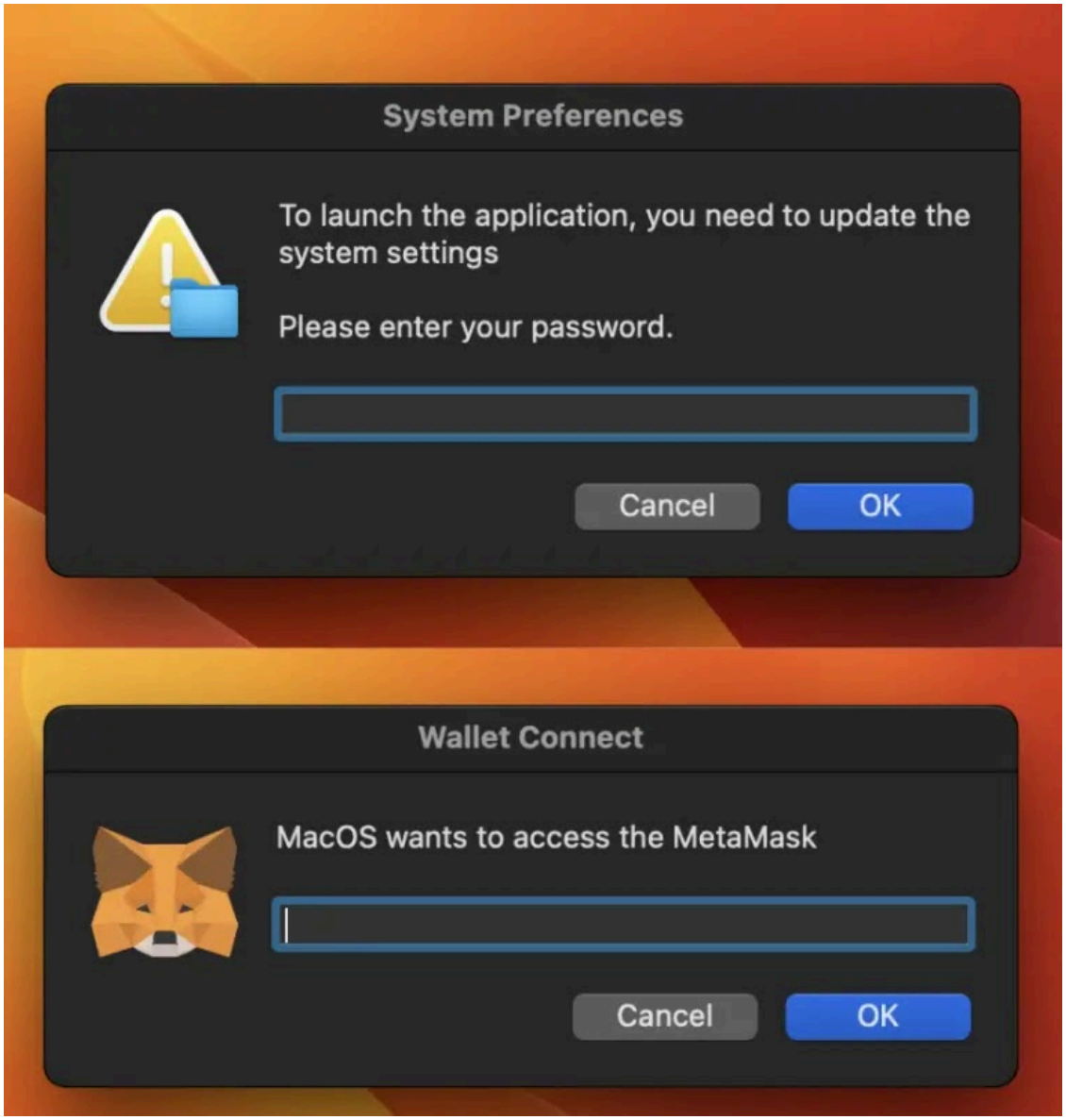
Poseidon Stealer Prompt (Source – Palo Alto Networks)

Cthulhu Stealer: Cthulhu Stealer is another prominent threat, sold via Telegram by the "Cthulhu Team." It is written in Go and distributed through malicious application installers.

Cthulhu Stealer targets a wide range of data, including browser credentials, cryptocurrency wallets, and files with specific extensions like `.png`, `.jpg`, and `.pdf`.

Cthulhu Stealer's Execution:-

Cthulhu Stealer uses fake dialog boxes to request passwords, including a MetaMask password. It saves stolen data in the `/Users/Shared/NW` directory and uploads it to a command-and-control server.



Cthulhu Stealer Fake Dialog (Source – Palo Alto Networks)

To combat these threats, organizations should implement advanced detection tools like Cortex XDR, which offers analytics for credential grabbing and sensitive information stealing.

These tools monitor unusual AppleScript executions and sensitive file access, helping identify malicious activities.

Implementing multi-layered defense strategies and staying informed about the latest threats are crucial steps in safeguarding sensitive information.

Indicators of Compromise (IoC):

- **SHA256 Hashes for Atomic Stealer:**
- `599e6358503a0569d998f09ccfbdeaa629d8910f410e26df0ffbd68112e77b05`
- `a33705df80d2a7c2deeb192c3de9e7f06c7bfd14b84f782cf86099c52a8b0178`
- **IP Addresses for Atomic Stealer C2 Servers:**
- `94.142.138[.]177`
- `194.169.175[.]117`
- **SHA256 Hashes for Poseidon Stealer:**
- `9f4f286e5e40b252512540cc186727abfb0ad15a76f91855b1e72efb006b854c`
- `5880430d86d092ac56bfa4aec7e245e3d9084e996165d64549ccb66b626d8c56`
- **IP Addresses for Poseidon Stealer C2 Servers:**
- `194.59.183[.]241`
- `70.34.213[.]27`

Tushar Subhra Dutta

Tushar is a Cyber security content editor with a passion for creating captivating and informative content. With years of experience under his belt in Cyber Security, he is covering Cyber Security News, technology and other news.