Understanding the threat of an AMOS

Threat

Atomic Stealer (AMOS)

Delivery

Malicious code is disguised as legitimate software.

Target

Exfiltrate credential data stored in Apple Keychain.

Attack

Compromised apps attack devices with malicious code.

Impact

Increased attack footprint extends threat actors’ access to unauthorized resources.

The anatomy of an AMOS

1.

Reconnaissance

Threat actors gain detailed information to compromise victims. Passive and active research ensures attack success.

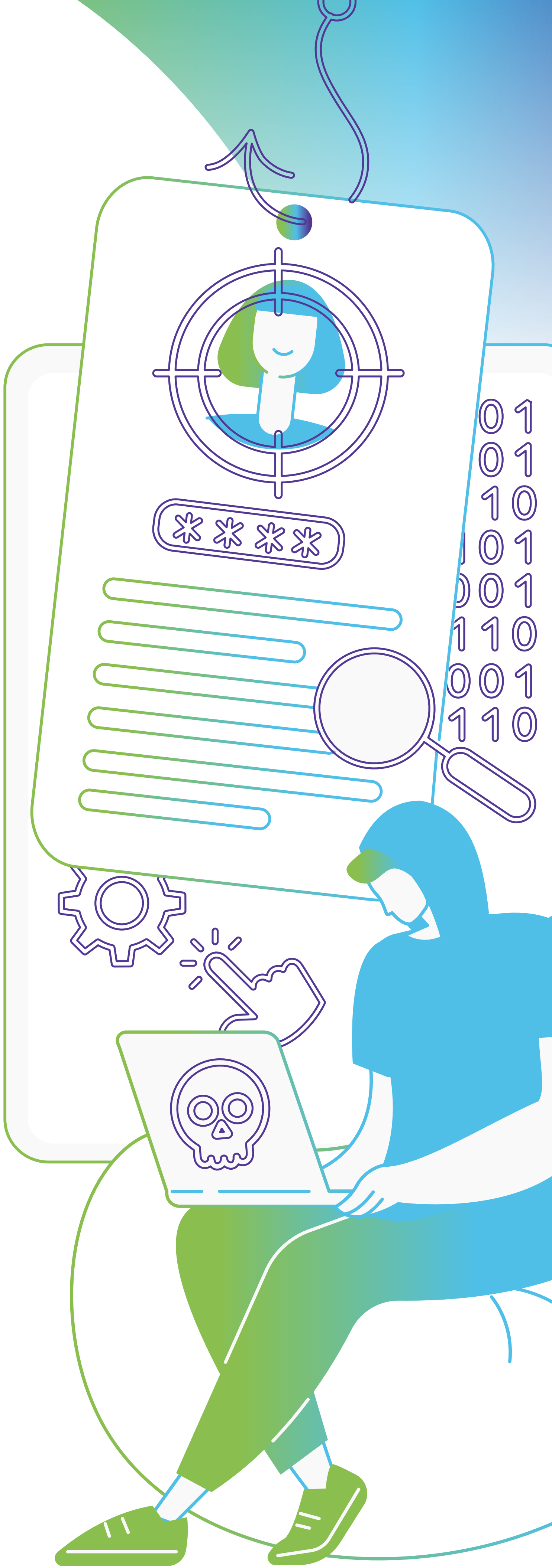
Example: Social engineering campaigns identify and befriend victims, gathering information to aid the attack's success.

2.

Weaponization

Intelligence gathered informs the development and customization of tools used to carry out the attack.

Example: Threat actors develop software, incoproate malicious code, and ad-hoc sign the package, making it ready for deployment to targets.



3.

Delivery

Research and tactics previously packaged are deployed to targets. AMOS relies on sponsored ads directing victims toward the imitation website where the infected app will be downloaded, compromising the computer at launch.

Example: The app runs malicious code in the background when the user executes the infected app.

4.

Exploitation

User credentials captured as part of a faked update prompt are used to exfiltrate confidential data from Apple Keychain.

Example: Types of data being gathered and exfiltrated:

- Usernames and passwords
- Browser session cookies
- Sensitive user data
- Payment card details
- Crypto wallets
- System metadata

5.

Installation

After a device is initially compromised, persistence tactics are deployed to maintain access to compromised devices.

Example: Threat actor creates a backdoor (like a hidden admin account) to continue extending the attack across the network.

6.

Command & Control (C2)

Threat actors use exfiltrated credentials to pivot attacks, stealing sensitive data from other resources.

Example: Threat actor puts the unauthorized access to use by gathering more data from networks and services. Using that data to:

- Expand attack footprint with greater access to data-rich resources
- Extend internal attacks through lateral movements
- Make more money by selling and/or extorting victims

7.

Actions on Objectives

As a result of gathering and exfiltrating credentials through AMOS, threat actors carry out the full breadth of their objectives. These actions are based in whole or in part on the unique objectives of the attacker.

Example: Some commonly seen objectives for attacks seen in the wild as a result of credential exfiltration are:

- Selling privacy data
- Supply chain attacks
- Theft of trade secrets
- Cyber terrorism
- Extortion
- Financial gain (crypto wallets)

Stats and other insightful nuggets about AMOS

- Infostealers, the malware category that AMOS falls under, are the most popular malware threat on macOS in 2023. (Objective-See)
- Atomic Stealer is #1 of the top 10 malware threats for macOS in 2024. (SentinelOne)
- Variant infostealers continue evolving to evade detection by XProtect and other system checks. (Dark Reading)
- Healthcare and financial services are the top 2 industries targeted by infostealing malware. (Forbes)
- Developers make Atomic Stealer available for rent as a Malware-as-a-Service (MaaS) solution to threat actors for $ 3,000 per month. (Hacker News)