Anatomy of an Atomic Stealer Attack

See how Atomic Stealer moves from social engineering to credential theft and follow-on compromise.

1

Reconnaissance

Threat actors gather information on targets to prepare the attack.

EXAMPLE: Social engineering campaigns identify and profile victims.

2

Weaponization

Attack tools are built and packaged using collected intelligence.

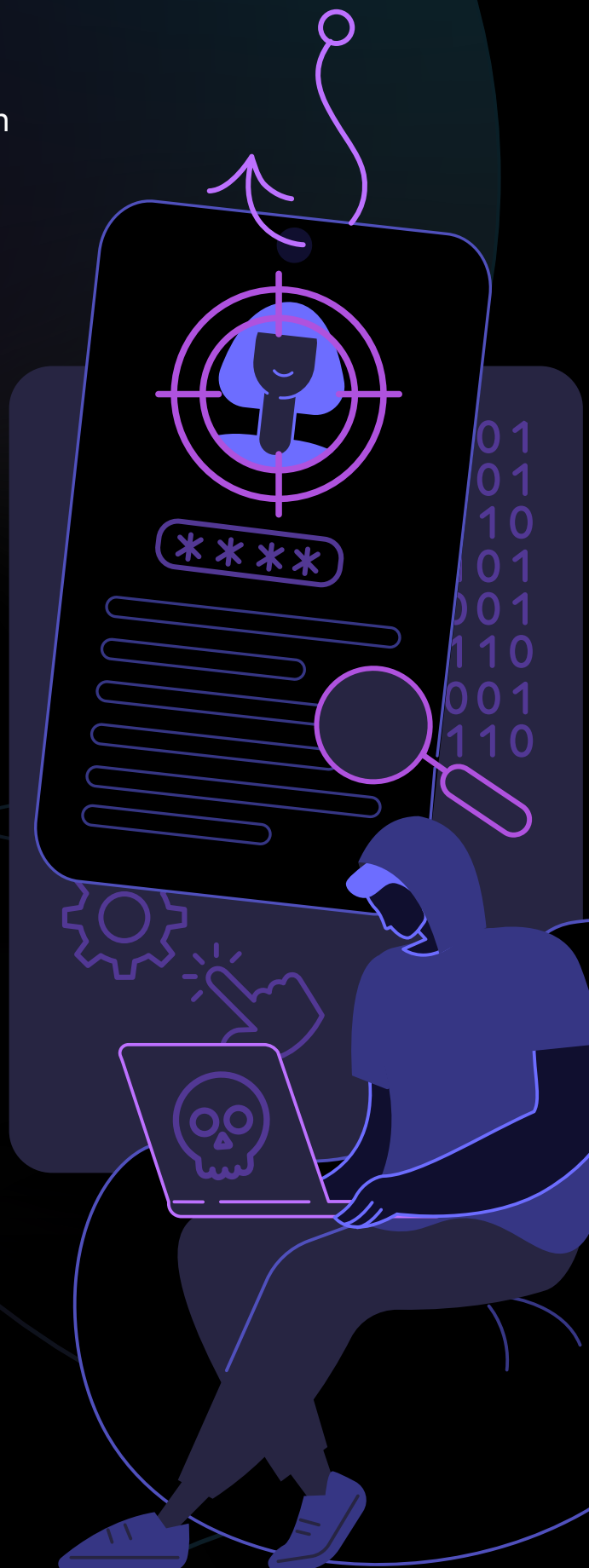
EXAMPLE: Malicious code is embedded into a legitimate-looking app.

3

Delivery

The malicious app is delivered through deceptive channels.

EXAMPLE: Sponsored ads lead users to download a fake app.



4

Exploitation

A fake prompt tricks the user into revealing credentials.

EXAMPLE: A spoofed update prompt captures login details and sensitive data.

5

Installation

Persistence mechanisms maintain access after initial compromise.

EXAMPLE: A hidden backdoor allows continued access to the device.

6

Command & Control (C2)

Stolen credentials are used to access additional systems and data.

EXAMPLE: Attackers use C2 to expand access and move across the network.

7

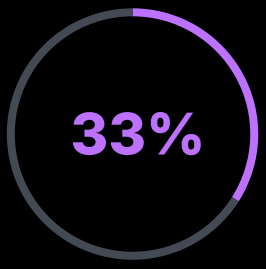
Actions on Objectives

Attackers use access to carry out broader compromise.

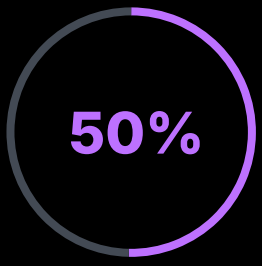
EXAMPLE: Account takeover, lateral movement, data theft and extortion.

jamf

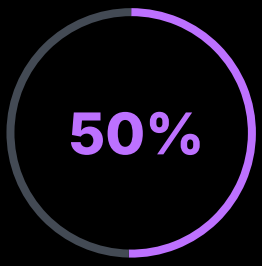
Why AMOS matters



infostealer-related malware



trojan-based attacks



of threats evade detection

SOURCE: Jamf Security 360: 2026 Annual Trends Report for Mac

Get the white paper