Atomic Stealer: What it is, how it hits macOS, and how to remove it

Gridinsoft Help Center

What it is

Atomic Stealer is macOS malware built to lift your secrets-especially crypto wallets, passwords, and browser data-then send them to attackers. It often looks harmless while it works. See behaviors and examples in the Atomic Stealer threat guide.

What you may notice

- New prompts asking for passwords or seed phrases
- Unknown browser extensions or profiles installed
- Unusual logins or crypto activity you didn’t make

How it gets in

- Fake app installers and cracked software
- Phishing sites posing as wallet tools or updates
- Malicious browser extensions

Remove it now (quick steps)

- Disconnect from the internet; don’t open wallets.
- Run a full scan with trusted anti-malware for macOS.
- From a clean device, change passwords and enable MFA.
- Move crypto to new wallets with fresh seed phrases; revoke suspicious approvals.
- On the Mac: remove unknown profiles, login items, LaunchAgents/Daemons, and extensions.

Prevent it

- Install software only from the App Store or the vendor’s site.
- Verify wallet tools; never enter seed phrases in a browser pop-up.
- Keep macOS, browsers, and extensions updated.
- Use a password manager + MFA on accounts.