A

Atomic Stealer (AMOS): macOS Infection, Detection, and Recovery

Atomic macOS Stealer targets browser data, passwords, files, and cryptocurrency. Cleanup must be followed by session revocation and wallet recovery.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

Atomic macOS Stealer, commonly called **AMOS** or **Atomic Stealer**, is an information-stealing malware family targeting macOS. It is distributed as malware-as-a-service, so different operators, campaigns, and forks may use different installers, infrastructure, filenames, and capabilities.

AMOS is not an Apple security warning or a legitimate component. It has been delivered through fake applications, cracked software, malicious advertisements, poisoned search results, and instructions that persuade users to paste commands into Terminal.

What Atomic Stealer can target

- browser passwords, cookies, autofill data, and active sessions;
- macOS Keychain data when the user supplies a system password;

- cryptocurrency wallet files, extensions, private keys, or seed phrases stored on the Mac;
- documents, desktop files, notes, messaging data, and system information;
- additional payloads or persistent backdoor access in some variants.

Moonlock reported a 2025 AMOS variant with persistent command execution, while its mid-2026 report notes that original operators became quieter but AMOS-derived code and forks remained. Do not assume every detection has identical behavior; investigate the observed sample and timeline.

How AMOS reaches a Mac

- trojanized DMG files impersonating utilities, wallets, productivity apps, or AI tools;
- fake “fix” instructions telling a user to copy a command into Terminal;
- installers that ask the user to bypass Gatekeeper or remove quarantine attributes;
- fake password prompts used to obtain the macOS account password.

A successful installation may produce no obvious slowdown. Unauthorized account activity or a security detection may appear only after data has already left the device.

Immediate response

1. **Disconnect the Mac.** Do not open financial accounts or wallets on it.
2. **Preserve details.** Record the installer, Terminal command, source URL, detection path, timestamps, and any password prompt.
3. **Scan and remove.** Use current macOS security software and update macOS. Inspect login items, profiles, browser extensions, LaunchAgents, LaunchDaemons, and unexpected applications based on verified findings—not a random filename list.
4. **Consider erasing the Mac.** A clean reinstall is appropriate when an administrator password was supplied, a persistent backdoor ran, security controls were changed, or the full payload cannot be established.

Secure accounts and cryptocurrency

From a known-clean device, revoke browser and application sessions before changing unique passwords. Prioritize email, password managers, Apple Account, work identity, financial services, exchanges, and accounts open in the browser during the exposure window. Re-enroll MFA and replace recovery codes when necessary.

If a wallet seed phrase or private key was stored, displayed, or entered on the infected Mac, create a new wallet with a new seed on a trusted device or hardware wallet and transfer remaining assets. Changing a wallet-app password does not rotate the blockchain private key. Review token approvals and exchange API keys.

Prevention

- Use the App Store or the publisher's manually verified official domain.
- Never paste an unexplained web command into Terminal to fix a browser or application problem.
- Do not disable Gatekeeper or quarantine protections for an unexpected installer.
- Keep valuable seed phrases off general-purpose computers and maintain versioned backups.

Atomic Stealer FAQ

Does deleting the DMG remove AMOS?

Only if it never ran. Once executed, the payload, stolen data, and persistence must be handled separately.

Will changing passwords on the infected Mac help?

It may expose the new credentials or session. Use a clean device after revoking active sessions.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com