

Forum:[Hack Forums](#)

Thread: [New macOS ClickFix attack silently mounts DMGs to push infostealer](#)

MadScientist - June 25, 2026, 8:37 pm

A new macOS ClickFix campaign is using Terminal commands to silently download, mount, and launch info-stealing malware from malicious disk image (DMG) files.

The campaign is infecting Mac devices with the Atomic macOS Stealer (AMOS) infostealer, which steals browser credentials, cryptocurrency wallet data, Keychain data, messaging app information, and user documents.

Researchers at Palo Alto Networks Unit 42 first discovered the campaign and say it begins with a fake CAPTCHA page that tells users to open Terminal and paste a malicious command to verify themselves.

Once executed, the command downloads a DMG file from an attacker-controlled server, silently mounts it with macOS's native hdiutil utility, locates the application bundle it contains, and launches it automatically.

ClickFix is a social engineering technique that displays fake CAPTCHAs, browser errors, or system alerts to trick visitors into copying and executing attacker-supplied "fix instructions." The technique has grown in popularity among threat actors in the past year and has been used by both cybercriminals and state-sponsored hacking groups to distribute malware.

While ClickFix attacks involving DMGs are not new, previous campaigns typically relied on users manually opening downloaded DMG files to launch malicious applications or execute scripts from attacker-controlled servers.

The campaign spotted by Palo Alto combines both approaches by using a Terminal command to quietly download a DMG file and launch the malware it contains.

After running the Terminal command, the attack downloads a malicious DMG from `svs-verificationdate[.]beer` using curl with the quiet "-fsSL" flags and saves it to the /tmp folder under a random filename.

The command then executes 'hdiutil attach -nobrowse' to mount the downloaded disk image without displaying it in Finder or on the desktop.

The script then searches up to three directory levels deep for the first available .app or .pkg installer, and if one is found, launches it using the macOS open command.

Researchers observed the malware being delivered as a disk image named "s.01M0td.dmg," which mounted a volume containing a self-signed application bundle named "NNApp.app."

This payload is part of the Atomic macOS Stealer family, which is used to steal credentials, browser history, authentication tokens, and cryptocurrency wallets from infected devices.

[Read More -](#)

<https://www.bleepingcomputer.com/news/security/new-macos-clickfix-attack-silently-mounts-dmgs-to-push-infostealer/>

Raijin - June 26, 2026, 2:20 pm

So the main takeaway is don't execute unknown terminal commands.