Smarttech
YOUR 24/7 SECURITY PARTNER

AmnesiaStealer macOS Malware Analysis

Executive Summary

AmnesiaStealer is a newly identified, Rust-based macOS infostealer, first documented by Jamf Threat Labs in August 2026. It is distributed through ClickFix-style social engineering: a fake GitHub download page tricks victims into pasting a Terminal command that installs the malware. It targets credentials, keychain material, browser data and cloud/crypto assets, and includes an on-demand module that gives an attacker live, hands-on-keyboard control of a victim's authenticated browser sessions.

The malware overlaps in objective with known families (Atomic/AMOS, MacSync, CrashStealer) but is distinguished by a builder-driven configuration and a dedicated remote-control second stage.

Initial Access & Infection Chain

AmnesiaStealer's delivery relies on a ClickFix lure rather than a conventional malicious installer, shifting the execution burden onto the victim and sidestepping macOS's built-in download and Gatekeeper protections.

Lure and social engineering

- Victims land on a spoofed GitHub-themed page featuring a "Download for macOS" button and a fake "Verified Publisher" badge intended to build false trust.
- Instead of serving an application, the page instructs the victim to open Terminal, paste a supplied command, and enter their macOS account password to "complete installation."
- The pasted command is base64-encoded to obscure its content, and retrieves a Stage 0 shell loader from attacker-controlled infrastructure.

Three-stage infection chain

Stage	Component	Function
Stage 0	Shell-script loader	Downloads a password-protected ZIP, extracts a universal Mach-O payload to /tmp under a hidden Apple-style filename, strips the quarantine attribute, applies an ad-hoc signature, runs the payload via nohup, then clears shell history.
Stage 1	Core infostealer (Rust, Mach-O)	Performs reconnaissance, harvests the local password, keychains, browser data, notes, documents and system data, then exfiltrates an archive to the C2 ("Amnesia Panel").
Stage 2	stream_module (remote-triggered)	Fetched only on operator command; clones and headlessly relaunches the victim's browser profile for live, interactive remote control.

Table 1: AmnesiaStealer's staged infection chain, as documented by Jamf Threat Labs.

Credential capture at install time

Once running, the payload performs basic host reconnaissance and mutes system sound, an evasive step intended to suppress the audible Finder chime normally heard when files are duplicated. It then displays a native-looking AppKit password dialog (styled as "Installer wants to make changes") to harvest the user's macOS account password, validating the entry locally before proceeding.

Notably, the captured password is written in cleartext to staging files, including a file at ~/.pwd, rather than being used only in memory, an operational-security weakness in the malware itself that can aid detection and forensic recovery.

Technical Analysis & Capabilities

Data collection scope

Following credential capture, AmnesiaStealer systematically collects a broad set of sensitive local data using standard file-copy utilities (cat, cp and duplicate for protected items), including:

- Login and data-protection keychains, including the per-host keychain file that holds cryptographic material tied to the device's hardware UUID.
- Chromium-based browser databases (login data, cookies, browsing history, bookmarks, extensions and local state) across up to sixteen supported Chromium-family browsers.
- Safari cookies and saved form values, subject to TCC access.
- Apple Notes content and attachments.
- Telegram session data.
- General documents and system/hardware profiling information.
- Cryptocurrency wallet browser-extension data.

Defence evasion and TCC bypass attempts

AmnesiaStealer attempts two Transparency, Consent and Control framework bypasses aimed at obtaining Safari cookie access and broader Full Disk Access, using a technique associated with an older, publicly known vulnerability (CVE-2020-9771). Jamf's analysis notes that on current macOS releases these bypass attempts largely fail, and the malware's own embedded debug logging records the failures, an indicator that the tooling has not been fully updated for modern macOS TCC protections. Where the host already holds Full Disk Access (for example, a developer's Terminal profile), the bypass is unnecessary and the theft proceeds regardless.

Safe Storage key manipulation

A further, more consequential behaviour was observed on hardened macOS versions: where the malware cannot recover a browser's existing Safe Storage encryption key from the keychain, it overwrites that key with a value already known to the operator. This does not recover historical data, but it silently re-keys future browser-saved passwords and cookies so that anything the browser stores from that point forward can be decrypted by the attacker, while remaining

unreadable to the legitimate user, a subtle, forward-looking form of persistence within the browser's own credential store.

Persistence and exfiltration

- Collected data is archived locally and exfiltrated to a command-and-control backend that the malware's own configuration refers to as the "Amnesia Panel".
- Persistence is achieved via a root LaunchDaemon disguised as an Apple crash-reporting component, following the naming pattern com.apple.ReportCrash.agent_<digits>.plist under /Library/LaunchDaemons/.
- The malware uses a builder-driven configuration model, meaning affiliates or operators can customise campaign parameters (lure branding, C2 endpoints, targeted data types) without recompiling the core binary, a RaaS-like operational pattern more commonly seen in ransomware tooling.

Advanced Features

Stream_module: live browser session hijacking

The most significant capability is a second-stage component, stream_module, fetched only when the C2 issues a remote_stream command. Rather than exporting stolen cookies for offline replay, it clones the victim's live Chromium profile, including its authenticated session state, into a hidden directory and relaunches it in a headless browser instance on the compromised host itself.

- The headless instance connects over the Chrome DevTools Protocol, giving the operator a live screencast of the session at roughly 3 frames per second.
- Full interactive input is supported: keyboard, mouse, scroll, page navigation and tab management, translated into CDP calls in real time.
- Because the session runs on the victim's own machine, the browser, host and network fingerprints (IP address, device identifiers, TLS/JA3 characteristics) are preserved, which helps the session evade anomaly-based and geo/device-mismatch fraud and access controls that would normally flag a login from a new location or device.
- Confirmed support spans multiple Chromium-based browsers, including Chrome, Edge, Brave, Arc, Opera and Vivaldi, all of which share the DevTools Protocol, comparable launch flags and cookie-encryption handling.
- Jamf's analysis also notes a stealth script bundled with this stage that patches browser fingerprinting APIs to avoid automation-detection flags on the sites the operator visits.

This turns a credential-theft event into a live account-takeover capability against any service the victim was logged into, including banking, e-mail, cloud storage and SSO-connected SaaS, and is very difficult to distinguish from genuine user activity using IP- or device-based controls alone.

OS version-branched logic

AmnesiaStealer's code branches its behaviour based on the detected macOS version, selectively attempting older, patched bypass techniques on legacy systems while adjusting its approach (such as the Safe Storage key overwrite) on current, hardened releases. This suggests the developers are actively tracking Apple's security changes and adapting rather than relying on a single static bypass chain, and implies unpatched or older enterprise Mac fleets carry materially higher exposure.

Family overlap and attribution context

Jamf notes that AmnesiaStealer's objectives overlap with established macOS infostealer families such as Atomic (AMOS), MacSync and CrashStealer, and that its distribution page reuses a template previously associated with the Atomic and MacSync campaigns. What differentiates it is the combination of a builder-driven configuration, OS-version-branched bypass logic, and the dedicated remote-control second stage, features that collectively point to a more mature, actively maintained toolkit rather than a one-off clone.

Recommendations

Strengthen preventive controls

1. Block execution of Terminal commands copied from clipboard where feasible.
2. Restrict or monitor unsigned/ad-hoc-signed Mach-O execution from /tmp, and alert on hidden files following the /tmp/.com.apple.dt.<digits> naming pattern.
3. Enforce macOS update compliance to macOS 26 baseline across all managed Mac fleets to close the TCC bypass path associated with CVE-2020-9771.
4. Apply least-privilege Full Disk Access grants; audit and revoke unnecessary Full Disk Access from Terminal and third-party apps.

Empower with risk awareness and preparedness

1. Brief employees and helpdesk staff specifically on ClickFix-style scams: never paste unknown Terminal commands from a website, regardless of how legitimate the page looks.
2. Include AmnesiaStealer-style scenarios (fake installer, Terminal paste, live session hijack) in the next macOS-focused tabletop exercise.
3. Review third-party browser extension and crypto-wallet usage policy on managed Mac endpoints, given the malware's targeting of wallet extension data.

Known Indicators of Compromise

The following indicators were published by Jamf Threat Labs in connection with the AmnesiaStealer campaign (August 2026).

Type	Indicator
Landing page	hxxps://github.aoitour[.]com
C2 / delivery	debug.allllowef[.]space
Related domain	news.allllowef[.]space

Type	Indicator
Related domain	shlyapadulina[.]space
Related domain	amz.shlyapadulina[.]space
Stage 1 SHA-256	de5748aac4a4d4cb48cf050652679e6bc49eda33d9ffaa0d280b578122fab55a
Stage 2 SHA-256	e853748ca8f9a5a9168263617409a9039ab09f4ffc7d860374c1e3b0b67b31a5
File artefact	/tmp/.com.apple.dt.<digits>
Persistence	/Library/LaunchDaemons/com.apple.ReportCrash.agent_<digits>.plist
Home artefact	~/.pwd

References

Jamf Threat Labs — AmnesiaStealer: macOS Infostealer That Hijacks Browsers

SecurityWeek — AmnesiaStealer macOS Malware Steals Data, Controls Browser Sessions

BleepingComputer — New AmnesiaStealer macOS malware hijacks browser sessions via remote control

GBHackers — New AmnesiaStealer Malware Targets macOS Users via ClickFix Attacks

SC Media — MacOS AmnesiaStealer malware spread through ClickFix, grants live browser control

CybersecurityNews — AmnesiaStealer macOS Malware Hijacks Browser Sessions via Fake GitHub Lure

MacTech — Jamf Threat Labs releases report of macOS malware dubbed 'AmnesiaStealer'

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com