INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-23 18:26 UTC

macOS ClickFix Automates DMG Delivery to Deploy AMOS Infostealer with Crypto Wallet Replacement

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0548
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	macOS; Browsers: Google Chrome, Microsoft Edge, Brave, Opera, Arc, Vivaldi, CocCoc, Yandex, Firefox, LibreWolf, SeaMonkey, Tor Browser, Waterfox, Zen Browser; Crypto Wallets: Exodus, Electrum, Atomic Wallet, Wasabi Wallet, Bitcoin Core, Litecoin Core, DashCore, Guarda, Binance Wallet, Dogecoin Wallet, TonKeeper, Ledger Live, Trezor Suite; Applications: Telegram Desktop, Discord, Apple Notes, Safari
Published	2026-06-23T14:30:16
Discovery Source	Rss

Executive Summary

A macOS-targeting campaign identified by Palo Alto Networks Unit 42 uses ClickFix-style social engineering to trick users into pasting a Terminal command that silently downloads, mounts, and executes a malicious disk image, delivering the Atomic macOS Stealer (AMOS) infostealer. The malware harvests browser credentials, cookies, cryptocurrency wallet contents, and macOS Keychain data, and replaces legitimate Ledger Live and Trezor Suite applications with trojanized versions to enable ongoing crypto theft. Organizations with macOS endpoints whose employees manage cryptocurrency assets, browser-stored credentials, or sensitive Keychain data face a high risk of credential exfiltration and sustained financial loss.

Technical Analysis

This campaign, attributed to an unknown threat actor and reported by Palo Alto Networks Unit 42 via BleepingComputer, uses the ClickFix social engineering technique on macOS. The victim is presented with a fake prompt instructing them to paste a Terminal command; that command automates the full DMG delivery chain, downloading, mounting via hdiutil, and executing the payload, without additional user interaction beyond the initial paste. The payload is Atomic macOS Stealer (AMOS), a well-documented infostealer targeting:

browser credential stores, cookies, and autofill data across Chrome, Edge, Brave, Opera, Arc, Vivaldi, CocCoc, Yandex, Firefox, LibreWolf, SeaMonkey, Tor Browser, Waterfox, and Zen Browser; cryptocurrency wallets including Exodus, Electrum, Atomic Wallet, Wasabi Wallet, Bitcoin Core, Litecoin Core, DashCore, Guarda, Binance Wallet, Dogecoin Wallet, and TonKeeper; macOS Keychain; and applications including Telegram Desktop, Discord, Apple Notes, and Safari. A distinguishing capability in this campaign is the replacement of Ledger Live and Trezor Suite with trojanized versions, enabling persistent wallet compromise and probable address-replacement or clipboard-hijacking for ongoing crypto theft post-infection. No CVE is assigned; the attack relies on user execution (MITRE T1204.002) rather than a software vulnerability. Relevant CWEs: CWE-522 (Insufficiently Protected Credentials), CWE-1021 (Improper Restriction of Rendered UI Layers), CWE-494 (Download of Code Without Integrity Check), CWE-693 (Protection Mechanism Failure). Key MITRE ATT&CK techniques include T1566 (Phishing), T1059.004 (Unix Shell), T1555/T1555.003 (Credentials from Password Stores/Web Browsers), T1539 (Steal Web Session Cookie), T1115 (Clipboard Data), T1036.005 (Match Legitimate Name or Location), T1041 (Exfiltration Over C2 Channel), and T1560 (Archive Collected Data). No patch is applicable; this is a user-execution-dependent campaign.

Action Checklist

1. Containment: Block macOS endpoints from downloading unsigned or unnotarized DMG files from the internet. Enforce macOS Gatekeeper and System Integrity Protection (SIP) via MDM policy on all managed macOS devices. Identify any macOS endpoints where users have administrative Terminal access and evaluate whether that access is necessary (NIST AC-6, Least Privilege).
2. Detection: Search endpoint logs and macOS Unified Logging for hdiutil commands invoked from Terminal by standard user accounts, especially within the same process chain as a browser session or curl/wget download. Hunt for unexpected DMG mount events followed by execution of unsigned binaries. Audit process creation logs for shell commands (bash/zsh) spawning download-and-execute chains. Review CIS 8.2, Collect Audit Logs: confirm macOS endpoint audit logging is enabled and forwarded to your SIEM.
3. Eradication: On any suspected host: remove mounted DMG volumes, quarantine and hash the DMG file for analysis, remove any applications installed from the DMG, and check Ledger Live and Trezor Suite installation paths for modified binaries (validate code signatures via codesign -v). Rotate all credentials accessible via the browser credential stores listed in the affected section. Users with crypto wallets on affected systems should treat wallet keys as compromised and transfer assets to new wallets with freshly generated keys.
4. Recovery: Reimage compromised macOS endpoints rather than attempting in-place remediation, given AMOS's Keychain access and application replacement capability. After reimaging, enforce CIS 7.3, Perform Automated Operating System Patch Management and CIS 7.4, Perform Automated Application Patch Management to restore to a verified clean baseline. Monitor post-recovery for outbound connections to C2 infrastructure and re-check browser credential stores after restoration.
5. Post-Incident: Conduct a user awareness exercise specifically covering ClickFix-style prompts: train users never to paste Terminal commands provided by websites or popups. Implement NIST AC-6, Least Privilege to restrict Terminal and administrative shell access on endpoints that do not require it. Review CIS 6.3, Require MFA for Externally-Exposed Applications and CIS 6.5, Require MFA for Administrative Access to reduce credential-reuse blast radius from harvested browser credentials. Evaluate D3-MFA and D3-CRO (Credential Rotation) as standing controls for all accounts whose credentials may have been browser-stored on affected devices.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if any macOS endpoint shows confirmed AMOS execution (unsigned binary run from a DMG mounted via hdiutil), confirmed Keychain or browser credential exfiltration, or if a user with a hardware crypto wallet (Ledger, Trezor) connected their device to a potentially compromised host — crypto asset theft is irreversible; additionally, if harvested credentials include access to regulated systems storing PII or PHI, breach notification obligations under applicable data protection law (e.g., CCPA, HIPAA, GDPR) must be evaluated with legal counsel.
Recovery Notes	Reimage all confirmed and suspected compromised macOS endpoints rather than attempting in-place cleanup, as AMOS replaces legitimate Ledger Live and Trezor Suite application bundles in-place, making binary-level trust of any installed application on the host unreliable. Post-reimage, monitor outbound network traffic for at least 72 hours against Unit 42's published AMOS C2 IOC list, and re-verify code signatures of all reinstalled crypto wallet applications before any hardware wallet is reconnected. Any user who had seed phrases, wallet.dat files, or crypto exchange credentials stored on an affected host should be treated as having those assets permanently at risk until funds are transferred to wallets generated on a clean, never-compromised device.
Forensic Artifacts	macOS Unified Log archive ('log collect --last 72h') showing hdiutil attach events with parent process tree tracing back to a browser or zsh/bash session spawned by a browser — the ClickFix delivery chain leaves a clear parent-child process ancestry in Unified Logging | Keychain database files at '~/Library/Keychains/login.keychain-db' and '~/Library/Keychains/default.keychain' — AMOS specifically targets these to harvest stored passwords, certificates, and secure notes; capture before any credential rotation | Browser Login Data SQLite databases at '~/Library/Application Support/Google/Chrome/Default/Login Data', '~/Library/Application Support/Microsoft Edge/Default/Login Data', and equivalent paths for each browser in the advisory (Brave, Opera, Arc, Firefox profile directory, etc.) — AMOS parses these directly for plaintext credential extraction | Ledger Live and Trezor Suite application bundle contents at '/Applications/Ledger Live.app/Contents/MacOS/' and '/Applications/Trezor Suite.app/Contents/MacOS/' — hash and codesign-verify these binaries; a trojanized version will have a mismatched or absent Apple Developer Team ID compared to the official vendor-signed binary | Crypto wallet data directories: Exodus at '~/Library/Application Support/Exodus/', Electrum at '~/.electrum/', Atomic Wallet at '~/Library/Application Support/atomic/', and Bitcoin Core wallet.dat at '~/Library/Application Support/Bitcoin/wallet.dat' — AMOS exfiltrates these directories wholesale; confirm whether any were accessed or modified by checking file system timestamps against the suspected compromise window

Per-Action IR Details

Containment — Block macOS endpoints from downloading unsigned or unnotarized DMG files from the internet. Enforce macOS Gatekeeper and System Integrity Protection (SIP) via MDM policy on all managed macOS devices. Identify any macOS endpoints where users have administrative Terminal access and evaluate whether that access is necessary (NIST AC-6 — Least Privilege).

NIST Phase: Containment
Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use Apple Configurator 2 or a free MDM trial (e.g., Mosyle free tier) to push a profile enforcing Gatekeeper at 'App Store and identified developers' minimum. For immediate network-level blocking without SIEM, create a DNS sinkhole entry or firewall ACL for known AMOS C2 domains published in Unit 42's threat bulletin. Use the macOS built-in command 'spctl --status' to verify Gatekeeper state on each host manually. For Terminal restriction, use 'dscl . -read /Groups/admin GroupMembership' to enumerate admin users and remove non-essential accounts with 'dseditgroup -o edit -d -t user admin'.

Evidence: Before enforcing MDM policy changes or revoking admin rights, capture volatile state: run 'ps aux | grep -E "hdiutil|bash|zsh|curl|wget"' to identify any in-progress AMOS execution chains; run 'hdiutil info' to enumerate currently mounted DMG volumes; capture 'netstat -an | grep ESTABLISHED' or 'lsof -i' to record active outbound connections that may indicate live AMOS exfiltration to C2. Capture the full macOS Unified Log stream for the past 24 hours with 'log collect --last 24h --output /tmp/unified_log.logarchive' before any MDM policy push alters log state. These volatile artifacts are destroyed once the host is isolated or the Terminal session is terminated.

Detection — Search endpoint logs and macOS Unified Logging for hdiutil commands invoked from Terminal by standard user accounts, especially within the same process chain as a browser session or curl/wget download. Hunt for unexpected DMG mount events followed by execution of unsigned binaries. Audit process creation logs for shell commands (bash/zsh) spawning download-and-execute chains. Review CIS 8.2 — Collect Audit Logs: confirm macOS endpoint audit logging is enabled and forwarded to your SIEM.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, enable macOS OpenBSM audit subsystem: edit '/etc/security/audit_control' to include 'ex,lo,aa,pc' flags and restart the audit daemon with 'audit -s'. Query the Unified Log directly with: 'log show --predicate "process == \"hdiutil\" OR process == \"bash\" OR process == \"zsh\"" --info --last 48h'. To detect ClickFix clipboard-paste execution chains, query for parent-child process relationships: 'log show --predicate "eventMessage CONTAINS \"hdiutil attach\"" --last 48h'. Use osquery with the query 'SELECT pid, parent, cmdline FROM processes WHERE cmdline LIKE "%hdiutil%" OR cmdline LIKE "%curl%dmg%";' to sweep all endpoints. A pre-built Sigma rule targeting macOS hdiutil execution from browser child processes can be converted to native Apple log queries using sigma-cli with the 'macos-log' backend.

Evidence: This is a detection/analysis step that does not alter live state, but evidence capture should be prioritized immediately: collect macOS Unified Log archives ('log collect --last 72h') from all suspect endpoints before any containment action flushes log buffers. Specifically hunt for log entries showing: (1) a browser process (Chrome, Safari, Brave, etc.) spawning a zsh/bash child; (2) that shell process invoking 'curl' or 'wget' to download a .dmg; (3) 'hdiutil attach' execution within the same process tree; (4) execution of an unsigned binary from '/Volumes/' mount paths. Also capture '/Library/Logs/DiagnosticReports/' for any crash dumps from AMOS execution failures, and check '~/Library/Application Support/' subdirectories for anomalous new entries corresponding to trojanized Ledger Live or Trezor Suite installs.

Eradication — On any suspected host: remove mounted DMG volumes, quarantine and hash the DMG file for analysis, remove any applications installed from the DMG, and check Ledger Live and Trezor Suite installation paths for modified binaries (validate code signatures via codesign -v). Rotate all credentials accessible via the browser credential stores listed in the affected section. Users with crypto wallets on affected systems should treat wallet keys as compromised and transfer assets to new wallets with freshly generated keys.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Before unmounting any DMG, hash it with 'shasum -a 256 /path/to/file.dmg' and quarantine a copy to an offline analysis system. Validate Ledger Live and Trezor Suite code signatures with 'codesign -v -v /Applications/Ledger\ Live.app' and 'codesign -v -v /Applications/Trezor\ Suite.app' — a trojanized binary will fail or show an unexpected Team ID. For browser credential rotation, use 'security find-generic-password -a -s ' to enumerate Keychain entries that AMOS targets; delete all browser-stored credentials and force re-authentication. For the crypto wallet transfer, instruct users to move assets from a clean, air-gapped device using a freshly generated seed phrase — never reuse the seed phrase that was present on the compromised host, as AMOS specifically harvests wallet.dat and seed phrase files from Exodus, Electrum, Atomic, and Wasabi paths.

Evidence: CRITICAL — volatile evidence must be captured BEFORE removing mounted DMGs, before killing any AMOS-related processes, and before rotating credentials. Capture: (1) full RAM acquisition using osxpmem or similar macOS memory acquisition tool to preserve any AMOS in-memory credential buffers or C2 beacon state; (2) 'hdiutil info' output listing all currently attached DMG volumes; (3) file hashes and metadata for any binaries dropped to '/tmp/', '/var/folders/', or '~/Library/Application Support/'; (4) a copy of the macOS Keychain database files at '~/Library/Keychains/' before credential rotation destroys the evidence of what was harvested; (5) browser credential store snapshots at '~/Library/Application Support/Google/Chrome/Default/Login Data' and equivalent paths for each affected browser listed in the advisory, before credentials are rotated. Failure to capture Keychain and browser stores before eradication will destroy forensic evidence of the full credential harvest scope.

Recovery — Reimage compromised macOS endpoints rather than attempting in-place remediation, given AMOS's Keychain access and application replacement capability. After reimaging, enforce CIS 7.3 — Perform Automated Operating System Patch Management and CIS 7.4 — Perform Automated Application Patch Management to restore to a verified clean baseline. Monitor post-recovery for outbound connections to C2 infrastructure and re-check browser credential stores after restoration.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), NIST AU-9 (Protection Of Audit Information)

Compensating: For teams without an automated imaging pipeline, use Apple Configurator 2 to restore macOS via DFU mode to a known-good IPSW, ensuring AMOS persistence mechanisms in LaunchAgents and LaunchDaemons are fully wiped. After reimaging, immediately reinstall Ledger Live and Trezor Suite directly from official vendor download pages only (ledger.com and trezor.io), and re-verify code signatures with 'codesign -v -v' before any user connects a hardware wallet. Post-recovery C2 monitoring can be accomplished with 'tcpdump -i en0 -w /tmp/postrecovery.pcap' running as a background job for 72 hours, with the capture reviewed against Unit 42's published AMOS C2 IOC list. Re-check browser credential stores 24 hours post-restoration with 'ls -la ~/Library/Application\ Support/Google/Chrome/Default/Login\ Data' to confirm no re-infection has occurred.

Evidence: Before reimaging, ensure all volatile and forensic evidence captured in prior phases has been preserved offline: RAM image, Keychain database copies, browser Login Data files, DMG hash and quarantined binary, Unified Log archive, and network connection snapshots. After reimaging, establish a clean-state baseline hash of Ledger Live and Trezor Suite application bundles using 'shasum -a 256 -r /Applications/Ledger\ Live.app/Contents/MacOS/Ledger\ Live' to enable future integrity verification. Retain pre-reimage forensic packages for a minimum of 90 days in case regulatory notification or legal hold requirements are triggered by confirmed credential or crypto asset theft.

Post-Incident — Conduct a user awareness exercise specifically covering ClickFix-style prompts: train users never to paste Terminal commands provided by websites or popups. Implement NIST AC-6 — Least Privilege to restrict Terminal and administrative shell access on endpoints that do not require it. Review CIS 6.3 — Require MFA for Externally-Exposed Applications and CIS 6.5 — Require MFA for Administrative Access to reduce credential-reuse blast radius from harvested browser credentials. Evaluate D3-MFA and D3-CRO (Credential Rotation) as standing controls for all accounts whose credentials may have been browser-stored on affected devices.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: For ClickFix-specific user training without a commercial awareness platform, create a one-page visual showing exactly what the AMOS ClickFix lure looks like — the fake CAPTCHA or verification prompt instructing users to open Terminal and paste a command — and distribute via email with a mandatory read-receipt. For Terminal restriction without MDM, use 'chmod 750 /bin/zsh /bin/bash' combined with group-based access controls as a stopgap, though MDM enforcement is strongly preferred. For MFA on browser-stored accounts, prioritize any SaaS applications, corporate email, and crypto exchange accounts confirmed to have had credentials stored in the affected browsers (Chrome, Edge, Brave, Firefox, and others listed in the advisory), using free TOTP implementations (e.g., Authy, Google Authenticator) where hardware keys are not available.

Evidence: Post-incident, compile a lessons-learned record documenting: (1) how many endpoints had unsigned DMG execution permitted by Gatekeeper misconfiguration or user bypass; (2) the full list of browser credential stores and Keychain entries confirmed or suspected to have been harvested by AMOS, cross-referenced with the browser list in the advisory; (3) whether any trojanized Ledger Live or Trezor Suite binaries were confirmed, indicating hardware wallet users who face ongoing crypto theft risk even post-remediation if they reconnected hardware wallets before reimaging. This record feeds directly into detection rule improvements: specifically, write a Sigma or osquery rule to alert on any future 'hdiutil attach' command executed from a browser child process or clipboard-paste Terminal session, ensuring this ClickFix delivery vector is permanently covered in the detection baseline.

Detection Guidance

Primary detection surface is macOS process execution and shell command logging. Hunt for: (1) hdiutil attach commands spawned from user-context shell processes, particularly when preceded by curl, wget, or osascript download activity within the same session; (2) zsh or bash processes executing unsigned binaries from /Volumes/ mount points; (3) codesign failures or missing signatures on Ledger Live or Trezor Suite binaries at their expected installation paths (/Applications/Ledger Live.app, /Applications/Trezor Suite.app); (4) unexpected writes to ~/Library/Keychains/ or access to browser profile directories (~/Library/Application Support/Google/Chrome, ~/Library/Application Support/Firefox/Profiles, etc.) by non-browser processes; (5) outbound HTTPS connections from newly spawned processes not matching known application baselines, particularly from processes running under /Volumes/ paths. In your SIEM, correlate macOS Unified Log events (category: process) with network flow data for the same host. IOC patterns from source material are not enumerated in available reporting; treat any unsigned DMG downloaded via Terminal command as high-confidence malicious. Reference CIS 8.2, Collect Audit Logs to confirm macOS audit logging is active before hunting.

Framework Mappings

MITRE-ATTACK

- **T1564.001** — Hidden Files and Directories
- **T1555** — Credentials from Password Stores
- **T1115** — Clipboard Data
- **T1539** — Steal Web Session Cookie
- **T1204.002** — Malicious File
- **T1027** — Obfuscated Files or Information
- **T1560** — Archive Collected Data

- **T1555.003** — Credentials from Web Browsers
- **T1543** — Create or Modify System Process
- **T1041** — Exfiltration Over C2 Channel
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1059.004** — Unix Shell
- **T1176** — Software Extensions
- **T1566** — Phishing

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **IA-5** — Authenticator Management
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **5.2** — Use Unique Passwords
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1564.001	Hidden Files and Directories	Defense-Evasion
T1555	Credentials from Password Stores	Credential-Access
T1115	Clipboard Data	Collection
T1539	Steal Web Session Cookie	Credential-Access
T1204.002	Malicious File	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1560	Archive Collected Data	Collection
T1555.003	Credentials from Web Browsers	Credential-Access
T1543	Create or Modify System Process	Persistence
T1041	Exfiltration Over C2 Channel	Exfiltration
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1059.004	Unix Shell	Execution
T1176	Software Extensions	Persistence
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-macos-clickfix-a...	T3
New macOS ClickFix attack silently mounts DMGs to push infostealer	https://www.bleepingcomputer.com/news/security/new-macos-clickfix-a...	T3
The Ultimate Browser Tier List - YouTube	https://www.youtube.com/watch?v=lGKonh65WiU	T3
Bitcoin Wallet Crypto Ethereum - Apps on Google Play	https://play.google.com/store/apps/details?id=io.atomicwallet&h...	T3

Source	URL	Tier
Edge - Crypto & Bitcoin Wallet - App Store - Apple	https://apps.apple.com/mo/app/edge-crypto-bitcoin-wallet/id1344400091	T3

Generated 2026-06-23 18:26 UTC by TJS Security Command Center