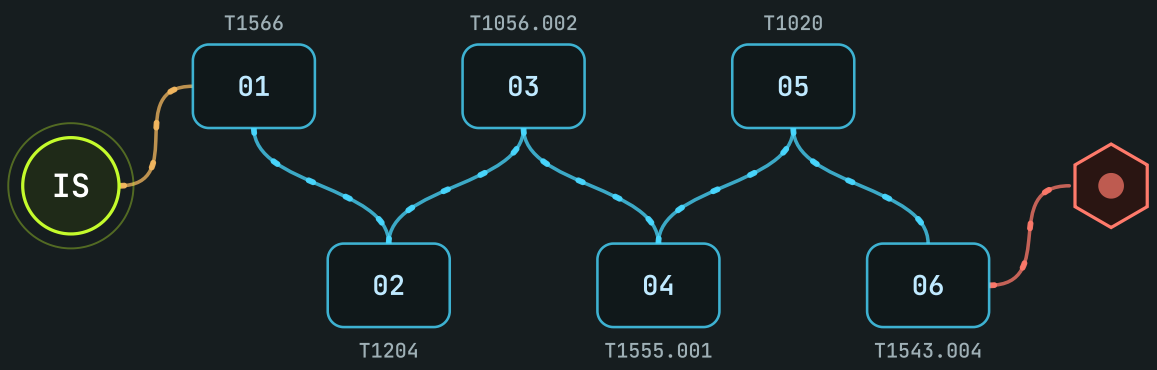


INTELLIGENCE BRIEF

Odyssey Stealer now leads macOS stealer detections and replaces wallet apps

Moonlock puts Odyssey at 62.7 percent of macOS stealer detections in early 2026. It now swaps wallet apps for drainers and takes cloud keys. Block Terminal paste lures, patch macOS and revoke sessions fast.

EDITION
Fall/Winter 2026/2027 Edition
IS-01 · Infostealer

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a glance

STATUS

ACTIVE

Odyssey accounted for 62.7 percent of macOS stealer detections in Moonlock's first-half 2026 telemetry, and no law enforcement action against it was found. [1]

HEADLINE NUMBERS

62.7%
of macOS stealer detections, first half of 2026 [1]

100+
countries with infections, per Moonlock in July 2026 [4]

about 300
wallet extension IDs targeted [4]

10
C2 hosts mapped across six autonomous systems [3]

KEY FACTS

INITIAL ACCESS
ClickFix pages: fake CAPTCHA or download, paste command into Terminal [2]

LINEAGE
AMOS fork, Poseidon rebrand; developer alias Rodrigo4 [3]

BUSINESS MODEL
Malware-as-a-service; 2023 forum ad priced $3,000 a month, 15 affiliates [3]

HARVESTS
Browser logins and cookies, Keychain, about 300 wallet extensions, 16 wallet apps, SSH and cloud keys [4]

PERSISTENCE
LaunchDaemon that polls the panel every 60 seconds, plus a Go-compiled SOCKS5 proxy [3]

INFRASTRUCTURE
10 C2 hosts across six autonomous systems in five countries [3]

02 What happened

The original edition, written in February 2026, tracked Odyssey as a fast-spreading ClickFix credential thief. By July 2026 Moonlock Lab was reporting infections in more than 100 countries, and its mid-year report put Odyssey at 62.7 percent of all macOS stealer detections. The stealer now replaces Ledger Live, Trezor Suite and Exodus with trojanized drainer builds and takes developer and cloud credentials alongside wallets and browser data.

- Moonlock Lab's July 2026 findings, reported by Cyber Security News and GBHackers, describe about 300 cryptocurrency wallet extension IDs and 16 desktop wallet applications in scope, up from the original edition's 203 and 18, plus SSH keys and AWS, Google Cloud, Azure and Docker configuration.
- Censys fingerprinted the Odyssey control panel and mapped 10 C2 hosts across six autonomous systems in five countries on February 11, 2026; later panels dropped the Odyssey name for a generic MacOS - Advanced Dashboard title.
- ClickFix is still the most common way in: Moonlock's first-half telemetry shows fake Homebrew, TradingView and LogMeIn lures, its October 2026 post citing Point Wild calls ClickFix the most popular technique on Macs, and in May 2026 it found three samples posing as a macOS build of OpenAI Codex that none of 72 engines detected a week after upload.
- Apple added a Terminal paste warning in macOS Tahoe 26.4 (released March 24, 2026) and shipped macOS Golden Gate 27 on September 14, 2026 with administrator controls that allow or deny executables by code-signing properties; XProtect reached version 5367 on October 13, 2026.
- Flare's analysis of 18.7 million 2025 stealer logs found Microsoft Entra ID credentials in 79 percent of enterprise identity logs and projected that one in five infections could expose enterprise credentials as early as the third quarter of 2026.
- No arrest, seizure or takedown tied to Odyssey or its developer was found. The June 2026 Operation Endgame phase neutralized 326 servers and 142 domains behind SocGholish, StealC and Amadey, not Odyssey.

03 How it works

01 Lure through ads and lookalike sites

MITRE ATT&CK T1566

Ads, search results and phishing steer users to pages impersonating Homebrew, TradingView, LogMeIn, Microsoft Teams or Ledger Live. Hunt.io tied 85 hostnames to one base64 installer pattern in October 2025.

02 ClickFix paste into Terminal

MITRE ATT&CK T1204

A fake CAPTCHA or install step tells the user to copy a base64 command and paste it into Terminal. The command pipes to bash, fetches a script with curl and runs AppleScript through osascript, so no traditional download is needed.

03 Fake password prompt

MITRE ATT&CK T1056.002

The script checks the typed password with dscl . authonly and, if it fails, shows a fake dialog headed Required Application Helper until the right password is entered. The password lets it unlock copied Keychain files.

04 Collect wallets, browsers and keys

MITRE ATT&CK T1555.001

It copies Keychain files, browser logins, cookies and autofill from Chromium browsers, Firefox and Safari, about 300 wallet extensions, 16 wallet apps, Apple Notes, Desktop and Documents files, SSH keys and cloud CLI configuration.

05 Zip and post to the panel

MITRE ATT&CK T1020

Everything is staged as out.zip under /tmp and sent by curl POST to the C2 /log endpoint with silent retries, then the staging files are removed.

06 Persist, proxy and replace wallets

MITRE ATT&CK T1543.004

A LaunchDaemon with a random com.<id>.plist label keeps an osascript loop polling the C2 every 60 seconds, a Go-compiled SOCKS5 proxy can turn the Mac into a relay, and Ledger Live, Trezor Suite and Exodus are killed, deleted and replaced with drainer builds that ask for PINs and recovery phrases.

04 Who is at risk

Anyone who runs a Mac and is used to pasting commands from the web is in scope; the operation avoids CIS countries and Moonlock reports infections in more than 100. The payoff is highest where one Mac holds wallet seeds, cloud keys or enterprise single sign-on.

- Software developers who install from Homebrew and follow Terminal instructions without a second look.
- Cryptocurrency holders and finance staff, the explicit target of the wallet extension list and the trojanized Ledger, Trezor and Exodus builds.
- Engineers whose Macs carry SSH keys and AWS, Google Cloud, Azure or Docker credentials, now harvested alongside browser data.
- Media, creative and education environments with high Mac adoption and thinner endpoint tooling.
- Any organization using Microsoft Entra ID, which Flare found in 79 percent of enterprise identity logs.

Sectors in scope: technology and software development, financial services and cryptocurrency, media and creative industries, education, remote and hybrid workforces.

05 What changed since the last edition

EACH CHANGE WITH ITS SOURCE

01 Scale and scope: Moonlock Lab reported Odyssey infections in more than 100 countries in July 2026, with about 300 wallet extension IDs and 16 desktop wallet apps in scope, plus SSH keys, AWS, Google Cloud, Azure and Docker configuration, FileZilla logins, Telegram and Discord data and shell history.

SOURCE 4

02 Market position: Moonlock's mid-2026 report puts Odyssey at 62.7 percent of macOS stealer detections against 29.8 percent for AMOS, says AMOS operators went quiet in late 2025, and found fake macOS builds of OpenAI Codex in May 2026 whose second stage matched Odyssey with zero detections a week after upload.

SOURCE 1

03 Wallet replacement became the headline capability: the malware kills and deletes Ledger Live, Trezor Suite and Exodus and downloads drainer builds that mimic the originals and prompt for PINs and recovery phrases.

SOURCE 5

04 Apple's Terminal paste warning in macOS Tahoe 26.4 did not hold: Moonlock's report says Jamf Threat Labs found a bypass that opens Script Editor through the applescript:// URL scheme, so the warning never fires, and adds that notarized does not mean safe because roughly one fifth of malicious Mach-O uploads carried valid or recently revoked Apple Developer certificates.

SOURCE 1

05 Infrastructure picture corrected: Censys's February 11, 2026 analysis maps 10 C2 hosts across six autonomous systems in the Netherlands, Germany, Singapore, Lithuania and Russia and names no registrant; the original edition's two-autonomous-system, Helsinki framing does not match the published research.

SOURCE 3

06 macOS Golden Gate 27 (September 14, 2026) lets administrators allow or deny executables by code-signing properties through declarative management, and Endpoint Security can terminate processes tied to a denied binary.

SOURCE 6

07 Current Apple baseline: macOS Golden Gate 27.0.1, Tahoe 26.7.1 and Sequoia 15.8.1 shipped September 28, 2026, and Tahoe 26.7.1 fixes a CoreGraphics out-of-bounds write (CVE-2026-86950) that Apple said may have been exploited in an extremely sophisticated attack against specific individuals on iOS versions before iOS 27.

SOURCE 7

08 No enforcement: no arrest, seizure or takedown tied to Odyssey or its developer was found as of October 2026; the June 15 to 19, 2026 Operation Endgame phase neutralized 326 servers and 142 domains behind SocGholish, StealC and Amadey.

SOURCE 8

06 What to do now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Teach every Mac user one rule: never paste a command from a web page, call or document into Terminal or Script Editor, and report any site that asks.**
ClickFix is the most common entry point and relies entirely on the user doing the work for the attacker.

02 **Move Macs to macOS Golden Gate 27.0.1 or Tahoe 26.7.1, keep XProtect current, and use the macOS 27 executable allow and deny rules to block unexpected binaries.**
Both builds shipped September 28, 2026, and the code-signing rules stop droppers and drainer builds before they run; do not rely on the Tahoe 26.4 Terminal paste warning, which has already been bypassed.

03 **Deploy EDR detections for osascript spawning curl, dscl . authonly after a password dialog, new plists in /Library/LaunchDaemons, shell archiving of Application Support folders and out.zip under /tmp.**
Hashes rotate per sample, while these behaviors recur across the Forcepoint, CloudSEK, Censys and SOC Prime analyses.

04 **Verify code signatures on Ledger Live, Trezor Suite and Exodus, alert on their deletion or replacement, and keep hardware wallet recovery phrases off any computer.**
The drainer builds look like the originals and ask for the PIN and seed; a hardware wallet cannot protect a seed typed into a fake app.

05 **On any suspected infection, revoke all browser sessions, reset passwords and rotate SSH keys, cloud CLI credentials, Docker and FileZilla secrets the same day.**
Odyssey takes session cookies that bypass MFA and now takes cloud and developer keys, so password resets alone leave access open.

06 **Enforce phishing-resistant MFA with short session lifetimes on Entra ID and other identity providers, and monitor stealer-log marketplaces for your domains.**
Flare found Entra ID credentials in 79 percent of enterprise identity logs and expects one in five infections to expose enterprise credentials from the third quarter of 2026.

07 **Block newly registered domains containing homebrew, macos, macapp, tradingview, ledger or teams at DNS, and treat ads for software downloads as untrusted.**
Hunt.io and Moonlock traced the campaigns to lookalike domains; Z7's 24/7 SOC and Microsoft 365 posture review cover the identity and endpoint layers described here.

07 Indicators

Indicators the sources publish, as they print them. Hunt with them, and check the source before you block.

IP	213.209.159[.]175 [3]
IP	62.60.131[.]230 [3]
IP	195.82.147[.]38 (second host presenting the same certificate) [11]
DOMAIN	homebrewclubs[.]org [11]

IP	62.60.131[.]250 [3]
IP	5.199.166[.]102 [3]
IP	77.90.185[.]24 [3]
IP	185.11.61[.]84 [3]
IP	217.119.139[.]117 [3]
IP	185.93.89[.]62 [3]
IP	185.93.89[.]63 [3]
IP	45.146.130[.]129 [3]
IP	45.146.130[.]131 (panel host in the August 2025 analysis) [9]
DOMAIN	something0x[.]at [3]
DOMAIN	charge0x[.]at [3]
DOMAIN	sdojifsfiudgigfiv[.]to [3]
DOMAIN	odyssey1[.]to [10]
DOMAIN	odyssey-st[.]com [10]
IP	165.245.215[.]18 (primary C2, July 2026) [4]
DOMAIN	rahtam[.]com (fallback C2, July 2026) [4]
DOMAIN	scubin[.]com (fallback C2, July 2026) [4]
IP	93.152.230[.]79 (phishing and payload backend, web and SSH active since September 2023) [11]
DOMAIN	homebrewfaq[.]org [11]
DOMAIN	homebrewonline[.]org [11]
DOMAIN	homebrewupdate[.]org [11]
DOMAIN	logmeln[.]com [11]
DOMAIN	logmeeine[.]com [11]
DOMAIN	tradingviewen[.]com [11]
DOMAIN	sites-phantom[.]com [11]
DOMAIN	filmoraus[.]com [11]
DOMAIN	teamsonsoft[.]com (fake Microsoft Teams download site) [12]
HASH	a0bdf6f602af5efea0fd96e659ac553e0e23362d2da6aecb13770256a254ef55 (AppleScript payload) [10]
HASH	d254125912d9e9e5c271766bc4f6eea0c296ad2c0cf19d4bd57081d1bf10f044 (Go-compiled SOCKS5 universal Mach-O, identical across C2s) [3]
FILE	/tmp/lovemrtrump/ staging directory [10]
FILE	/tmp/out.zip [9]
FILE	/Library/LaunchDaemons/com.<5-digit number>.plist with KeepAlive and RunAtLoad set [3]
BEHAVIOR	osascript spawning curl; ditto or zip of Application Support directories; shell writing to /Library/LaunchDaemons; HTTP POST to /log [13]
BEHAVIOR	osascript -e 'run script' alongside dscl . authonly and a fake dialog headed Required Application Helper (CloudSEK YARA rule OSX_Odyssey_Osascript_Exec) [12]
BEHAVIOR	Panel HTML title MacOS - Advanced Dashboard (earlier Odyssey - Advanced Dashboard) [3]
BEHAVIOR	Censys query: host.services.threats.name: "Odyssey Stealer" or web.threats.name: "Odyssey Stealer" [3]

08 Sources

[1] **Moonlock's mid-2026 macOS threat report** Moonlock Lab · July 16, 2026. https://moonlock.com/mid-2026-macos-threat-report

[2] **New Wave of Odyssey Stealer Targets macOS Users in Active Cyberattack Campaign (reporting Moonlock Lab, February 5, 2026)** GBHackers · February 6, 2026. https://gbhackers.com/odyssey-stealer/

[3] **Odyssey Stealer: Inside a macOS Crypto-Stealing Operation** Censys · February 11, 2026. https://censys.com/blog/odyssey-stealer-inside-a-macos-crypto-stealing-operation/

[4] **Odyssey Stealer Hits macOS Users in 100+ Countries, Targets 300 Crypto Wallet Extensions (reporting Moonlock Lab)** Cyber Security News · July 10, 2026. https://cybersecuritynews.com/odyssey-stealer-hits-macos-users/

[5] **Odyssey Stealer Attacks Macs Worldwide and Replaces Crypto Wallet Apps With Drainers (reporting Moonlock Lab, July 8, 2026)** GBHackers · July 10, 2026. https://gbhackers.com/odyssey-stealer-attacks-macs/

[6] **Apple overhauls security with iOS and macOS 27** iTnews · September 15, 2026. https://www.itnews.com.au/news/apple-overhauls-security-with-ios-and-macos-27-628916

[7] **macOS 27.0.1, Tahoe 26.7.1 and Sequoia 15.8.1 security content** 9to5Mac · September 28, 2026. https://9to5mac.com/?p=1071773

[8] **Operation Endgame continues: international coalition takes malware offline** Eurojust · June 24, 2026. https://www.eurojust.europa.eu/news/operation-endgame-continues-international-coalition-takes-malware-offline

[9] **Odyssey Stealer: ClickFix Malware Attacks macOS Users for Credentials and Crypto Wallet Details** Forcepoint X-Labs · August 7, 2025. https://www.forcepoint.com/blog/x-labs/odyssey-stealer-attacks-macos-users

[10] **Odyssey Stealer: The Rebrand of Poseidon Stealer** CYFIRMA · June 26, 2025. https://www.cyfirma.com/?p=43744

[11] **Odyssey Stealer & AMOS Hit macOS Developers with Fake Homebrew Sites** Hunt.io · October 16, 2025. https://hunt.io/blog/macos-odyssey-amos-malware-campaign

[12] **Threat Actors Impersonate Microsoft Teams to Deliver Odyssey macOS Stealer via ClickFix** CloudSEK · September 5, 2025. https://www.cloudsek.com/blog/threat-actors-impersonate-microsoft-teams-to-deliver-odyssey-macos-stealer-via-clickfix

[13] **Odyssey Stealer: macOS Crypto Wallet Theft via MaaS** SOC Prime · February 13, 2026. https://socprime.com/active-threats/odyssey-stealer-analysis/

[14] **Apple has released an update to XProtect for all macOS (version 5319)** The Eclectic Light Company · October 15, 2025. https://eclecticlight.co/2025/10/15/apple-has-released-an-update-to-xprotect-for-all-macos-18/

[15] **Apple has released an update to XProtect for all macOS (version 5326)** The Eclectic Light Company · January 22, 2026. https://eclecticlight.co/2026/01/22/apple-has-released-an-update-to-xprotect-for-all-macos-24/

[16] **How XProtect is hunting scripts** The Eclectic Light Company · February 5, 2026. https://eclecticlight.co/2026/02/05/how-xprotect-is-hunting-scripts/

[17] **XProtect update listing (version 5367 on October 13, 2026; version 5329 on February 10, 2026)** The Eclectic Light Company · October 13, 2026. https://eclecticlight.co/tag/xprotect/

[18] **Apple iOS Zero-day Vulnerability Exploited in Attacks (CVE-2026-20700)** Qualys ThreatProtect · February 12, 2026. https://threatprotect.qualys.com/2026/02/12/apple-ios-zero-day-vulnerability-exploited-in-attacks-cve-2026-20700/

[19] **New MacSync macOS stealer uses signed and notarized dropper to bypass Gatekeeper (reporting Jamf Threat Labs)** The Hacker News · December 24, 2025. https://thehackernews.com/2025/12/new-macsync-macos-stealer-uses-signed.html

[20] **Apple security releases** Apple · page published September 28, 2026. https://support.apple.com/en-us/100100

[21] **This cyberattack tricks you into hacking yourself (reporting Microsoft Digital Defense Report 2025)** ZDNET (via Yahoo Tech) · October 17, 2025. https://tech.yahoo.com/cybersecurity/articles/cyberattack-tricks-hacking-yourself-heres-140100241.html

[22] **Flare Research Warns 1 in 5 Infostealer Infections Could Yield Enterprise Credentials in 2026** Flare · February 2, 2026. https://flare.io/company/press/flare-research-warns-1-in-5-infostealer-infections-could-yield-enterprise-credentials-in-2026

[23] **ATT&CK versions** MITRE · v20.0 released April 28, 2026. https://attack.mitre.org/resources/versions/

[24] **Q3 data shows infostealers and trojans now dominate Mac malware (reporting Point Wild)** Moonlock Lab · October 9, 2026. https://moonlock.com/q3-malware-report-infostealers-trojans

[25] **Apple has released an update to XProtect for all macOS (version 5325)** The Eclectic Light Company · December 16, 2025. https://eclecticlight.co/2025/12/16/apple-has-released-an-update-to-xprotect-for-all-macos-23/

NEXT STEP

Put the same team on your environment

Talk to the team that runs the Z7 Solutions™ SOC about what this brief means for your environment. We will tell you what applies and what does not.

ALSO IN THIS EDITION

- Qilin still tops most ransomware counts
  More from the edition · z7solutions.com/z7-cyber/qilin/
- Qilin still hits hospitals and infrastructure
  More from the edition · z7solutions.com/z7-cyber/qilin-part-2/
- LockBit 5.0 returns after Operation Cronos
  More from the edition · z7solutions.com/z7-cyber/lockbit/

CALL	844-974-8669
EMAIL	sales@z7solutions.com
BOOK A CALL	z7solutions.com/book/

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.