Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

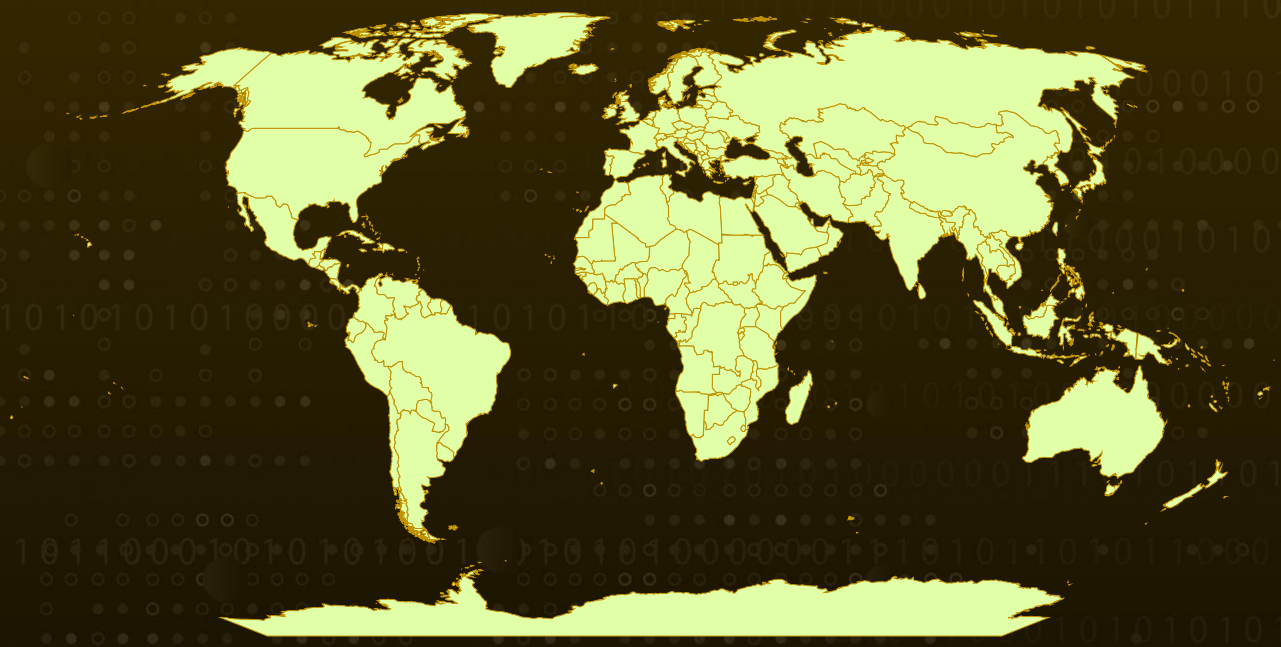
Fake CAPTCHA, Real Theft: macOS ClickFix Drains Crypto Wallets

Date of Publication	Admiralty Code	TA Number
August 07, 2026	A1	TA2026224

Summary

First Seen: March 2026
Targeted Regions: Worldwide
Targeted Platform: macOS
Targeted Products: Apple Keychain, cryptocurrency wallets (Bitcoin, Litecoin, Dogecoin, Monero, Ethereum, XRP)
Attack: A ClickFix lure is being used to trick macOS users into pasting a command into Terminal that quietly installs a Go-based stealer. Once running, the malware harvests browser passwords, Apple Keychain data, and cached credentials, then goes after cryptocurrency wallets, redirecting balances to attacker-controlled addresses. What sets it apart is that it does not always empty a wallet outright; it can siphon off only a set percentage at a time to avoid drawing attention. All of the supporting infrastructure traces back to a sanctioned Russian bulletproof hosting provider.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

A Go-based stealer is being actively pushed through ClickFix attacks against macOS users, quietly siphoning cryptocurrency funds, browser-saved passwords, Apple Keychain entries, and cached credentials. The intrusion begins when the victim receives an email carrying a link, and once the page loads, a popup dressed up as a routine CAPTCHA check instructs them to copy a block of text and paste it into the Terminal. That single pasted line quietly reaches out to an attacker-controlled server, pulls down a first-stage shell script, runs it, and then wipes the Terminal window and clears the command history so the victim sees no trace of what just happened.

#2

The downloaded script acts as a profiler and loader. It fingerprints the machine, gathering hardware identifiers, memory details, the processor architecture, and the name of the logged-in account, then uses that architecture check to fetch the matching build of the payload. Before running it, the script creates a folder whose name imitates a legitimate Apple certificate-validation process, drops the payload inside under a trustworthy-looking name, marks it executable, and strips the quarantine flag that macOS normally uses to warn users about files downloaded from the internet. The payload itself is a Go-based stealer, obfuscated to hide its inner workings, that ships in separate versions for Apple Silicon and Intel Macs. It settles in for the long term by registering itself as a background launch agent through the operating system's own task-management framework, disguised as a software-update helper.

#3

To gain the access it needs, the malware throws up a convincing fake password prompt built from a native scripting tool, tricking the victim into handing over their account credentials so it can make further changes without asking again. From there it sweeps the disk for anything valuable, matching files by name and extension to locate browser password databases, Apple Keychain contents, and cached credentials sitting in browser cookies.

#4

Harvested secrets are sent out to an attacker-run command-and-control server over plain HTTP on an unusual port. The most distinctive piece is a wallet-draining routine that checks whether a cryptocurrency address has a balance and, if it does, redirects the funds to wallets controlled by the attacker. Rather than emptying an account in one move, it can pull off only a set percentage at a time, calculating what each slice is worth to stay under the radar. It reaches across Bitcoin, Litecoin, Dogecoin, Monero, Ethereum, and XRP, and every stage of the operation- loader hosting, payload delivery, and command-and-control- traces back to Aeza Group, a Russian bulletproof hosting provider sanctioned by the US, UK, and Australia.

#5 ClickFix has fueled a steady stream of campaigns against Windows users, delivering a broad mix of malware from backdoors to loaders and infostealers. Its use here to plant a native macOS payload shows the same social-engineering trick being pointed at a wider set of targets.

Recommendations

- **Train Users to Spot ClickFix Lures:** Teach staff that no legitimate website or CAPTCHA ever asks them to copy a command and paste it into the Terminal. Any prompt that does is an attack, and the safe response is to close it and report it.
- **Establish a Rapid Reporting and Isolation Path:** Make sure users know to alert IT immediately if they run one of these commands, and have a process to pull the affected Mac into network isolation before the stealer can finish exfiltrating data or draining wallets.
- **Deploy Script-Blocking Browser Controls:** Roll out script-mitigation add-ons such as NoScript to cut down on the fake CAPTCHA popups that kick off the ClickFix chain.
- **Filter Malicious Domains and Hosting at the Network Edge:** Block the ClickFix staging domain and sinkhole known-bad domains at the DNS layer, and block the attacker-controlled IP addresses tied to this activity outright.
- **Block Sanctioned Bulletproof Hosting Ranges:** Deny inbound and outbound traffic to the Aeza Group address space used for loader delivery, payload hosting, and command-and-control, since legitimate business traffic to these ranges is unlikely.
- **Rotate Exposed Credentials and Reset the Keychain:** On any Mac suspected of infection, assume browser-stored passwords and Keychain contents are compromised, reset those credentials, and revoke active sessions.
- **Protect Cryptocurrency Holdings:** Move funds from any potentially exposed hot wallet, favor hardware wallets for storage, and independently verify destination addresses before signing transactions, as this malware can quietly alter transactions before they are approved.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
Execution	T1204: User Execution	T1204.001: Malicious Link
	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Discovery	T1082: System Information Discovery	
	T1033: System Owner/User Discovery	
Defense Evasion	T1070: Indicator Removal	T1070.003: Clear Command History
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1027: Obfuscated Files or Information	
Persistence	T1543: Create or Modify System Process	T1543.001: Launch Agent
Credential Access	T1056: Input Capture	T1056.002: GUI Input Capture
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
Collection	T1005: Data from Local System	

Tactic	Technique	Sub-technique
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1571: Non-Standard Port	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f0062f7e70e61493684a2f60748a475168e155bc2502163c844c42e87692abd0, 619a99ba4ee9d7f33db8045c7e03c4265424977993fe8a53b0f45157c5abd3e5, 5bad988affc1094f12b8b8bed659ef55b20e2988eb25441e1c1b34dd03b3eb52, b43a909a01e954d6549558f2f7e9bb58e34959a0ae229f340d61091ab726bbd3
File Path	HOME/Library/Caches/com.apple.trustd/com.apple.verified, HOME/Library/Caches/homeenergyd/com.apple.homeenergyd
IPv4	193[.]29[.]224[.]151, 77[.]221[.]152[.]34, 138[.]124[.]118[.]69
IPv4:Port	138[.]124[.]118[.]69[:]8133
Domain	profitnow[.]io

References

https://www.huntress.com/blog/mac-crypto-draining-malware

https://www.hivepro.com/threat-advisory/clickfix-campaigns-deliver-babadeda-lorem-ipsum-and-potemkin-loaders

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

August 07, 2026 • 07:50 AM

More at www.hivepro.com