Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

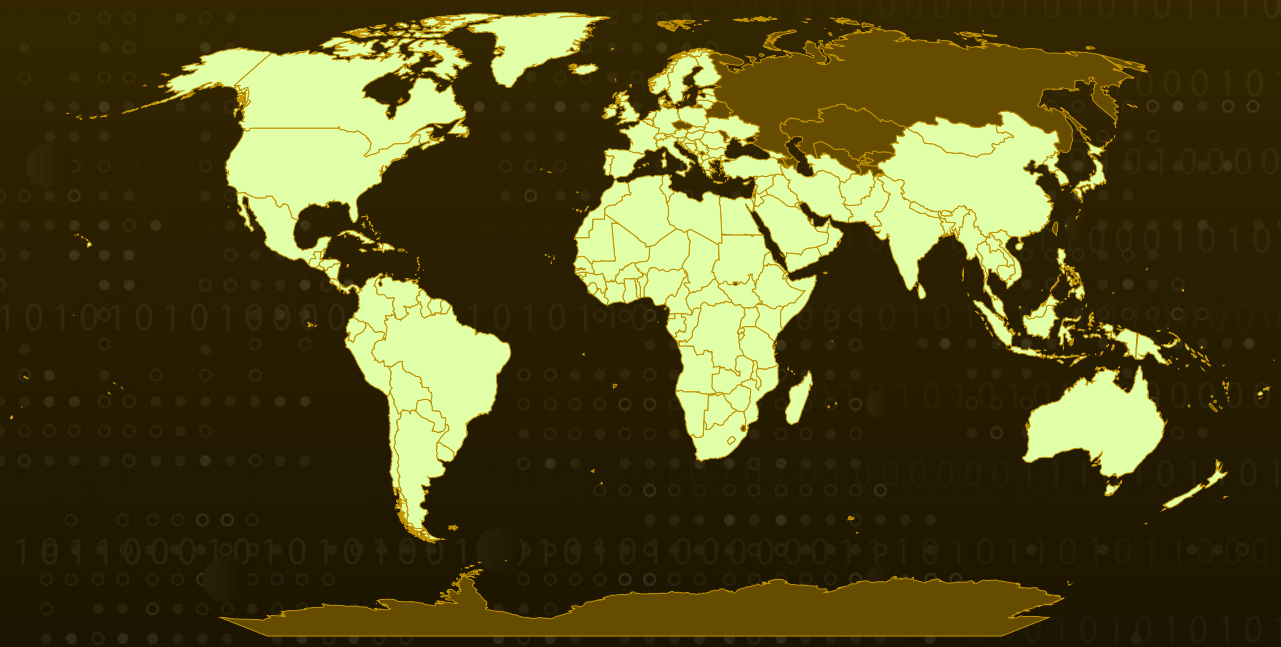
Fake Homebrew ClickFix Campaign Delivering Cuckoo Stealer on macOS

Date of Publication	Admiralty Code	TA Number
February 19, 2026	A1	TA2026050

Summary

First Seen: January 13, 2026
Targeted Regions: Global (excludes CIS countries)
Targeted Platforms: macOS
Targeted Industries: Software Development, Technology, Cryptocurrency
Malware: Cuckoo Stealer
Attack: A social engineering campaign leverages the ClickFix technique to deliver Cuckoo Stealer, a full-featured macOS infostealer and remote access trojan, through typosquatted Homebrew installation pages. Attackers created high-fidelity clones of the legitimate Homebrew website (brew.sh) across multiple domains hosted on shared infrastructure, tricking macOS developers into executing a modified curl command that downloads a credential-harvesting loader followed by a second-stage infostealer binary capable of exfiltrating browser credentials, cryptocurrency wallets, Keychain data, messaging sessions, and more.

Attack Regions



Targeted Non-Targeted

Attack Details

#1

A social engineering campaign is targeting macOS users by impersonating the official Homebrew package manager website and weaponizing developer trust. Victims are funneled to typosquatted domains through search engine poisoning, malicious advertisements, and deceptive look-alike URLs. The threat actors have built near pixel-perfect clones of the legitimate Homebrew site, carefully replicating its branding, layout, and multilingual functionality. The deception hinges on a subtle modification within the installation command: instead of pulling from raw.githubusercontent.com, the script references raw.homabrews[.]org, a minor alteration that can easily evade casual inspection. A JavaScript-powered "Copy" button silently places the malicious curl command into the user's clipboard, exploiting the common developer workflow of pasting installation commands directly into Terminal.

#2

Once executed, the tampered command retrieves a trojanized installer script from the attacker-controlled domain. Malicious logic is injected into what appears to be the standard Homebrew installation routine. The first-stage payload focuses on credential harvesting, repeatedly prompting the user for their macOS password. It leverages the native dscl utility with the authonly argument to validate credentials without creating a login session or generating authentication logs. Failed attempts return a convincing "Sorry, try again" message, mimicking normal sudo behavior. After obtaining valid credentials, the script downloads a secondary binary named brew_agent into /tmp, Base64-encodes the stolen password, and passes it as a parameter. This stage deploys Cuckoo Stealer, which initializes command-and-control communications, generates a unique session identifier, collects environment data, and removes the macOS quarantine attribute via xattr to suppress Gatekeeper warnings. It also performs locale-based filtering to avoid systems configured for CIS regions and uses custom XOR-based string obfuscation with rotating keys to evade static detection.

#3

To maintain persistence, the malware abuses the macOS LaunchAgent mechanism, registering itself as com.homebrew.brewupdater.plist to blend in as a legitimate Homebrew component. The binary is copied into a hidden directory such as .local-{session_id} under the name BrewUpdater. Command-and-control traffic is encrypted over HTTPS using X25519 elliptic curve Diffie–Hellman key exchange, generating ephemeral key pairs to derive shared secrets for session encryption. The malware implements a compact RAT protocol that supports arbitrary shell execution, silent command execution, system reboot, self-destruct routines with LaunchAgent cleanup, and granular exfiltration controls. Commands are transmitted as single-byte identifiers within a pipe-delimited beacon structure and encrypted using XOR keys derived from MD5 hashes.

#4

Cuckoo Stealer's data exfiltration capabilities are extensive and financially motivated. It silently captures screenshots using the macOS screencapture -x utility and establishes a secondary socket channel for interactive file browsing. Before sensitive activity, it mutes system audio via AppleScript to reduce user awareness. Browser credential theft targets Chromium-based browsers, extracting cookies, saved logins, autofill records, browsing history, bookmarks, and installed extensions particularly cryptocurrency wallet extensions such as Coinbase Wallet, Phantom, Binance Wallet, and Rabby. The malware also exfiltrates the macOS Keychain directory, Apple Notes databases, Discord tokens, Telegram session data, FileZilla credentials, OpenVPN profiles, Steam session files, and wallet data from over twenty cryptocurrency applications, including node wallets for Bitcoin, Litecoin, Dogecoin, Raven, and DashCore demonstrating a deliberate focus on harvesting high-value financial assets at scale.

Recommendations

- **Verify Homebrew Installation Sources:** Always verify the legitimacy of Homebrew installation commands by confirming the source URL before executing any curl-based installation command in Terminal. Bookmark the legitimate brew.sh website to avoid reliance on search engine results.
- **Block Known Malicious Infrastructure:** Immediately block the identified malicious domains (homabrews[.]org, brewsh[.]cx, brrewsh[.]org, brewshh[.]org, brewmacos[.]com) and IP address 5.255.123[.]244 at the DNS, proxy, and firewall levels across all organizational endpoints.
- **Audit macOS LaunchAgents for Unauthorized Persistence:** Review all LaunchAgent plists in ~/Library/LaunchAgents/ for suspicious entries, specifically checking for com.homebrew.brewupdater.plist or any plist referencing binaries in hidden directories matching the pattern ".local- " within the user home directory.
- **Deploy Endpoint Detection Rules for Credential Harvesting:** Create detection rules for processes invoking the dscl command with the authonly verb outside of expected authentication workflows, as this indicates potential credential harvesting activity consistent with this campaign's first-stage payload.

Enforce Browser Extension Whitelisting: Implement browser extension whitelisting policies to protect cryptocurrency wallet extensions (Coinbase Wallet, Phantom Wallet, Binance Wallet, Rabby Wallet) from unauthorized Local Storage and IndexedDB access by malicious processes.

Rotate Credentials on Suspected Compromised Hosts: If evidence of compromise is found, immediately rotate all credentials stored in macOS Keychain, browser password managers, FTP clients (FileZilla), VPN configurations (OpenVPN), and messaging application sessions (Discord, Telegram), as Cuckoo Stealer targets all of these data stores.

Implement DNS Monitoring for Typosquatted Domains: Deploy DNS monitoring solutions capable of detecting typosquatting patterns targeting commonly used developer tools and package managers, with automated alerting for domains that closely resemble legitimate software distribution infrastructure.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1608: Stage Capabilities	T1608.005: Link Target
Initial Access	T1566: Phishing	T1566.002: Spearphishing Link
	T1189: Drive-by Compromise	
Execution	T1204: User Execution	T1204.002: Malicious File
		T1204.004: Malicious Copy and Paste
		T1204.001: Malicious Link
	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
		T1059.002: AppleScript
Persistence	T1543: Create or Modify System Process	T1543.001: Launch Agent
	T1547: Boot or Logon Autostart Execution	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
	T1070: Indicator Removal	T1070.004: File Deletion
	T1656: Impersonation	

Tactic	Technique	Sub-technique
Discovery	T1614: System Location Discovery	T1614.001: System Language Discovery
	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1518: Software Discovery	
Credential Access	T1056: Input Capture	T1056.002: GUI Input Capture
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
	T1539: Steal Web Session Cookie	
Collection	T1113: Screen Capture	
	T1005: Data from Local System	
	T1119: Automated Collection	
	T1560: Archive Collected Data	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
		T1573.001: Symmetric Cryptography
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1529: System Shutdown/Reboot	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f985cd667c77e7d99c1ac2ea9cb0861ded15e1c2d44e480cbd178ca8b2caae42, 545dd5cba264bf242bc837330ca34247e202f7ac25f03eec63bf5842357519f1
Path	~/Library/LaunchAgents/com.homebrew.brewupdater.plist, ~/.local-{session_id}/BrewUpdater
Domains	homabrews[.]org, raw[.]brewsh[.]cx, braw[.]sh, brewsh[.]cx, brew[.]lat, brew[.]pages[.]dev, brrewsh[.]org, brewmacos[.]com
IPv4	5[.]255[.]123[.]244

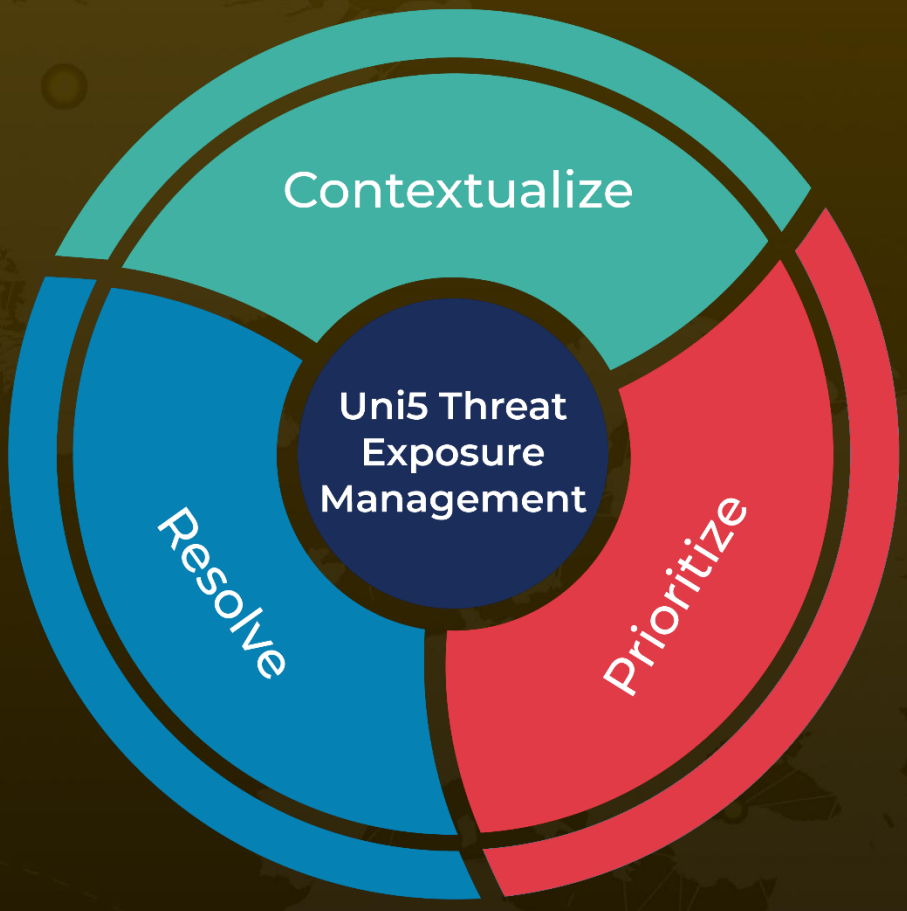
References

https://hunt.io/blog/fake-homebrew-clickfix-cuckoo-stealer-macos

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 19, 2026 • 8:30 AM

More at www.hivepro.com