Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

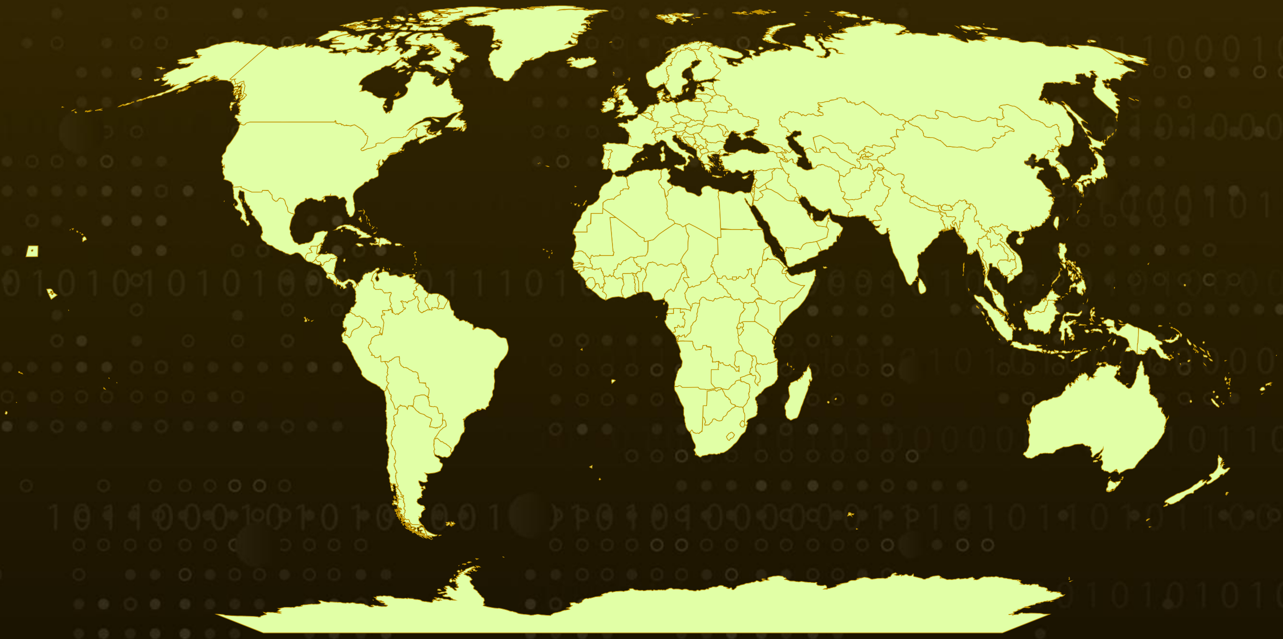
Atomic Stealer Targeting Mac Users via Malicious GitHub Pages

Date of Publication	Admiralty Code	TA Number
September 23, 2025	A1	TA2025293

Summary

First Seen: September 2025
Targeted Region: Worldwide
Malware: Atomic Stealer (AMOS)
Affected Platform: macOS
Attack: A recent campaign is targeting macOS users by abusing GitHub Pages and SEO to distribute Atomic stealer (AMOS) malware. Attackers create sites impersonating trusted software vendors, tricking users into pasting malicious Terminal commands that fetch and run hidden payloads. Once installed, the stealer harvests credentials, browser data, and crypto wallets, exfiltrating them to attacker-controlled servers. Users are advised to avoid running commands from untrusted sources, verify the origin of GitHub repos before downloading anything, and reset important credentials from a clean device if they suspect exposure.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

A new campaign is targeting macOS users by abusing GitHub Pages and SEO manipulation to distribute malware. Attackers create repositories and web pages impersonating well-known software vendors, making them appear legitimate in search engine results. These fraudulent sites lure users into clicking "Install on Mac" buttons, which redirect to malicious landing pages containing instructions to paste commands into the Terminal.

#2

The supplied commands use tools like curl to fetch and execute obfuscated scripts, which ultimately install Atomic stealer (AMOS), a known macOS information-stealing malware. Once active, Atomic stealer can harvest browser data, saved credentials, cryptocurrency wallet information, and other sensitive files, exfiltrating them to attacker-controlled infrastructure.

#3

The campaign is not limited to a single brand or service. Multiple impersonated vendors have been observed, suggesting a broad and organized effort to compromise users across different sectors. The attackers continuously rotate GitHub accounts and repository names to bypass takedowns, which makes the campaign persistent and harder to block through simple domain controls.

#4

Defenders are advised to monitor for suspicious GitHub Pages activity, block identified malicious domains, and investigate endpoints for evidence of unusual curl or shell activity. End-users should be reminded never to copy and run Terminal commands from unverified websites and to only obtain software through official vendor sites or trusted app stores. If compromise is suspected, affected systems should be isolated, credentials reset from a clean device, and a full reinstallation considered to ensure removal of the stealer.

Recommendations

Avoid Running Unverified Commands: Never copy and paste commands into the Terminal from websites or emails unless you fully trust the source. Malicious scripts can install malware, steal credentials, or create persistent threats. Always verify the origin of any command before executing it.

Download Software from Trusted Sources: Only install software from official vendor websites or verified app stores. Avoid third-party download links, GitHub Pages, or search-engine results that may be impersonating legitimate software. This minimizes the risk of installing malicious payloads.

Monitor for Suspicious Activity: Watch for unusual system behavior, such as unexpected applications, repeated prompts for credentials, or abnormal network traffic. Early detection of anomalies can prevent sensitive information from being stolen. Use endpoint monitoring tools where available.

Protect Credentials and Enable MFA: If there's any chance a device has been exposed, immediately change passwords and security keys from a separate, secure device. Enable multi-factor authentication (MFA) on all critical accounts to add an extra layer of security.

Isolate and Remediate Infected Systems: Disconnect suspected Macs from the network to prevent data exfiltration. Investigate for downloaded malware, check for persistence mechanisms, and consider a full macOS reinstall to ensure complete removal of Atomic stealer.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0006 Credential Access	TA0009 Collection	T1555 Credentials from Password Stores	T1005 Data from Local System

T1608.006 SEO Poisoning	**T1608** Stage Capabilities	**T1566** Phishing	**T1204** User Execution
T1059 Command and Scripting Interpreter	**T1059.004** Unix Shell	**T1036** Masquerading	**T1204.002** Malicious File
T1027 Obfuscated Files or Information	**T1189** Drive-by Compromise		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e52dd70113d1c6eb9a09eafa0a7e7bcf1da816849f47ebcdc66ec9671eb9b350, 943788d7e478575440e09a196b33fc772b289409fe70990024aac88aa1a3def8
MD5	f202824cb3f89d7e5d0145b9ddcd958d
Domains	lorissarenfro[.]com, cfocares[.]com
URLs	hxxp://github[.]com/lastpass-on-macbook, hxxp://github[.]com/LastPass-on-MacBook/lastpass-premium-mac-download, hxxp://ahoastock825[.]github[.]io/.github/lastpass, hxxp://macprograms-pro[.]com/mac-git-2-download.html, hxxp://bonoud[.]com/get3/install.sh, hxxp://bonoud[.]com/get3/update, hxxp://github[.]com/Zengo-Wallet-Desktop-App-on-Macbook, hxxp://github[.]com/1password-on-Macbook-Desktop, hxxp://github[.]com/1Password-Premium-on-MacBook, hxxp://github[.]com/ActiveCampaign-Desktop-on-Mac, hxxp://github[.]com/ActiveCampaign-MacBook-Desktop-App, hxxp://github[.]com/After-Effects-Desktop-on-Mac, hxxp://github[.]com/Audacity-on-Macbook,

TYPE	VALUE
URLs	hxxp://github[.]com/Auphonic-Desktop-on-Mac, hxxp://github[.]com/Basecamp-App-macOS-Installation, hxxp://github[.]com/BetterSnapTool-on-MacBook, hxxp://github[.]com/Biteable-Desktop-on-Mac, hxxp://github[.]com/Bitpanda-on-MacBook, hxxp://github[.]com/Bitsgap-Download-Mac, hxxp://github[.]com/Blog2Social-Desktop-on-Mac, hxxp://github[.]com/Blue-Wallet-Desktop-on-Mac, hxxp://github[.]com/Bonkbot-On-Macbook, hxxp://github[.]com/Carbon-Copy-Cloner-on-MacBook, hxxp://github[.]com/Carbon-Copy-Cloner-on-MacBook, hxxp://github[.]com/Charles-Schwab-Desktop-on-MacBook, hxxp://github[.]com/Citibank-on-MacBook-Desktop-App, hxxp://github[.]com/CMC-Markets-on-MacBook, hxxp://github[.]com/Confluence-on-MacBook, hxxp://github[.]com/Coolors-Desktop-on-Mac, hxxp://github[.]com/DaVinci-Resolve-on-MacBook, hxxp://github[.]com/DefiLlama-on-Mac-Desktop-App, hxxp://github[.]com/Desktop-Clockology-Mac-Os, hxxp://github[.]com/Desygner-Desktop-on-Mac, hxxp://github[.]com/Docker-MacBook-Desktop-App, hxxp://github[.]com/Dropbox-on-Macbook, hxxp://github[.]com/EigenLayer-Desktop-App-on-MacBook, hxxp://github[.]com/EigenLayer-Desktop-App-on-MacBook, hxxp://github[.]com/EigenLayer-Desktop-App-on-MacBook, hxxp://github[.]com/E-TRADE-on-MacBook, hxxp://github[.]com/Fidelity-on-MacBook, hxxp://github[.]com/Fliki-Desktop-on-Mac, hxxp://github[.]com/Freqtrade-Bot-on-Macbook, hxxp://github[.]com/Freshworks-App-on-MacBook, hxxp://github[.]com/Gemini-on-MacBook, hxxp://github[.]com/GMGN-AI-Desktop-App-On-MacBook, hxxp://github[.]com/Gunbot-Desktop-on-Macbook, hxxp://github[.]com/Hemingway-Editor-Desktop-on-Mac, hxxp://github[.]com/HeyGen-Desktop-on-Mac, hxxp://github[.]com/Hootsuite-MacBook-Desktop-App, hxxp://github[.]com/HTX-App-on-MacBook-Download, hxxp://github[.]com/Hypertracker-Desktop-on-Mac, hxxp://github[.]com/IRS-Desktop-App-on-Macbook, hxxp://github[.]com/KeyBank-on-Mac-Desktop, hxxp://github[.]com/Lightstream-Desktop-on-Mac, hxxp://github[.]com/Loopback-on-MacBook, hxxp://github[.]com/Maestro-Bot-Desktop-on-Macbook, hxxp://github[.]com/Melon-Desktop-on-Mac,

TYPE	VALUE
URLs	hxxp://github[.]com/Metatrader-5-Download-on-Mac, hxxp://github[.]com/Metricool-Desktop-on-Mac, hxxp://github[.]com/Mixpanel-on-MacBook, hxxp://github[.]com/Mp3tag-Desktop-on-Mac, hxxp://github[.]com/Mural-App-on-MacBook, hxxp://github[.]com/NFT-Creator-on-Macbook, hxxp://github[.]com/NotchNook-Download-on-Mac, hxxp://github[.]com/Notion-Download-on-Mac, hxxp://github[.]com/Obsidian-on-Macbook, hxxp://github[.]com/Onlypult-Desktop-on-Mac, hxxp://github[.]com/Pendle-Finance-Desktop-on-Mac, hxxp://github[.]com/Pepperstone-on-MacBook, hxxp://github[.]com/Pipedrive-on-Mac-Desktop-App, hxxp://github[.]com/Plus500-on-MacBook, hxxp://github[.]com/Privnote-on-MacBook, hxxp://github[.]com/ProWritingAid-Desktop-on-Mac, hxxp://github[.]com/Publer-Desktop-on-Mac, hxxp://github[.]com/Raycast-App-on-Mac, hxxp://github[.]com/Raycast-Download-on-Mac, hxxp://github[.]com/Reaper-Desktop-on-Mac, hxxp://github[.]com/RecurPost-Desktop-on-Mac, hxxp://github[.]com/Renderforest-Desktop-on-Mac, hxxp://github[.]com/Rippling-App-on-MacBook, hxxp://github[.]com/Riverside-fm-Desktop-on-Mac, hxxp://github[.]com/Robinhood-Desktop-on-MacBook, hxxp://github[.]com/Rug-AI-on-Macbook, hxxp://github[.]com/Sage-Intacct-on-Mac-Desktop-App, hxxp://github[.]com/Salesloft-on-MacBook, hxxp://github[.]com/SentinelOne-on-MacBook, hxxp://github[.]com/Shippo-on-MacBook, hxxp://github[.]com/Shopify-on-MacBook, hxxp://github[.]com/SocialPilot-Desktop-on-Mac, hxxp://github[.]com/Soundtrap-Desktop-on-Mac, hxxp://github[.]com/StreamYard-Desktop-on-Mac, hxxp://github[.]com/SurferSEO-Desktop-on-Mac, hxxp://github[.]com/Thunderbird-on-MacBook, hxxp://github[.]com/TweetDeck-Desktop-on-Mac, hxxp://github[.]com/Uphold-App-on-MacBook, hxxp://github[.]com/Uphold-App-on-MacBook, hxxp://github[.]com/Veeva-CRM-on-MacBook, hxxp://github[.]com/Viraltag-Desktop-on-Mac, hxxp://github[.]com/VSCO-Desktop-on-Mac, hxxp://github[.]com/Vyond-Desktop-on-Mac, hxxp://github[.]com/Webull-on-Macbook, hxxp://github[.]com/Xai-Games-App-on-MacBook, hxxp://github[.]com/XSplit-Desktop-on-Mac

References

https://blog.lastpass.com/posts/attack-targeting-macs-via-github-pages

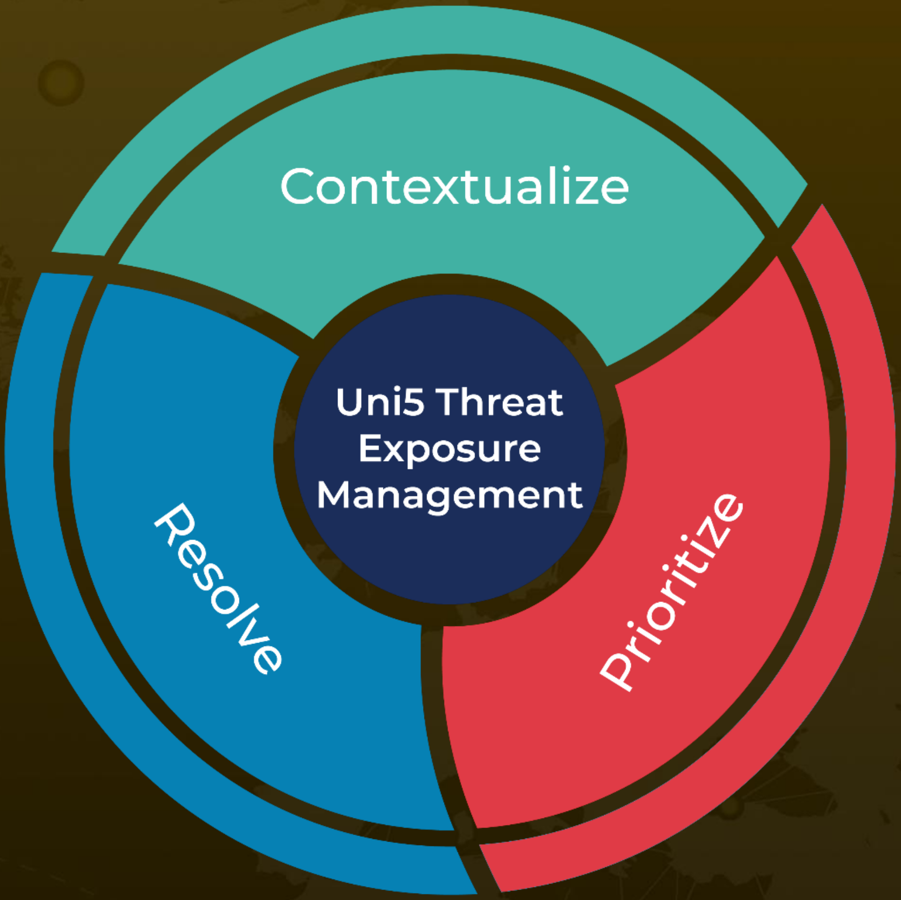
https://medium.com/deriv-tech/brewing-trouble-dissecting-a-macos-malware-campaign-90c2c24de5dc

https://hivepro.com/threat-advisory/clickfix-scam-targets-macos-with-amos-malware/

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

September 23, 2025 • 11:00 AM

More at www.hivepro.com