Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

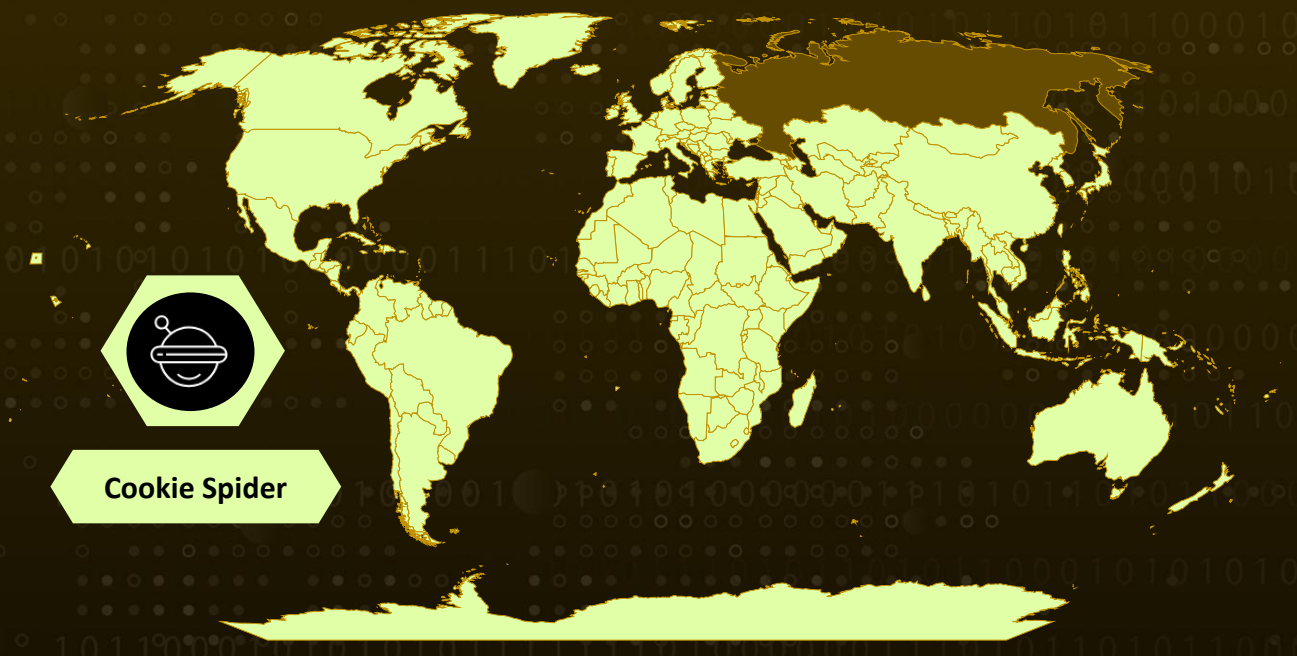
New SHAMOS Stealer Exploits One-Line Commands on macOS

Date of Publication	Admiralty Code	TA Number
August 26, 2025	A1	TA2025259

Summary

Attack Began: June 2025
Targeted Region: Worldwide (Except Russia)
Threat Actor: Cookie Spider
Malware: SHAMOS (Atomic Stealer variant)
Affected Platform: macOS
Attack: A recent campaign by the cybercriminal group COOKIE SPIDER deployed SHAMOS, a variant of the Atomic macOS Stealer (AMOS), to target users through malvertising and fake support websites. Victims were tricked into running one-line terminal commands that downloaded the malware, which used evasion techniques, bypassed Apple's Gatekeeper, and stole sensitive data such as credentials, browser information, and crypto wallets. SHAMOS also established persistence and sometimes delivered additional malicious payloads disguised as legitimate apps, showcasing the growing sophistication of macOS-targeted threats.

Attack Regions



Attack Details

#1

A recent campaign deployed a macOS-focused malware known as SHAMOS, a variant of the Atomic macOS Stealer (AMOS) operated by the cybercriminal group COOKIE SPIDER. Active between June and August 2025, the campaign primarily relied on malvertising and fraudulent support websites to ensnare victims. Users searching for troubleshooting help were lured to fake sites that instructed them to run one-line terminal commands, which secretly downloaded and executed SHAMOS.

#2

Once on a system, SHAMOS used a variety of methods to bypass defenses and remain undetected. It carried out anti-VM checks to evade sandboxing, removed Apple Gatekeeper attributes from files, and leveraged AppleScript to gather reconnaissance on the host system. Its data theft capabilities focused on browser credentials, Keychain entries, crypto wallet data, and notes, which it packaged into archives and exfiltrated via remote servers. In some cases, it also installed additional payloads masquerading as legitimate applications, such as fake versions of Ledger Live.

#3

The campaign had a wide global reach, with the U.S., UK, Japan, China, Colombia, Canada, Mexico, and Italy identified as the most targeted countries. This geographic spread highlights the broad ambitions of the attackers, who leveraged a scalable delivery model that could reach victims across multiple continents.

#4

By blending social engineering with simple but effective technical tricks, such as malvertising combined with one-line install commands, the operators demonstrated how macOS users remain a lucrative target for credential theft and financial fraud. The campaign also underscores the growing sophistication and adaptability of macOS malware families like AMOS, which continue to evolve with new variants and delivery tactics.

Recommendations

Educate Users on Malvertising Risks: Train employees and end users to recognize suspicious ads, fake support pages, and prompts to run terminal commands from unverified sources. Emphasize that legitimate troubleshooting rarely requires copy-pasting complex one-liners directly from unknown websites.

Restrict Execution of Unsigned Scripts: Configure systems to block or alert on execution of unsigned scripts and binaries, especially those fetched via curl, wget, or similar tools. Monitoring for bash -c or obfuscated commands (such as Base64 decoding) can help spot malicious activity early.

Strengthen Endpoint Monitoring: Deploy endpoint monitoring rules to detect behaviors linked to information-stealing malware. Examples include unusual use of xattr to modify file attributes, AppleScript execution from unexpected directories, and repeated access to Keychain or browser credential stores.

Network and Data Exfiltration Controls: Watch for abnormal outbound traffic patterns, such as repeated curl uploads, compressed archive transfers, or connections to newly registered or suspicious domains. Implement data loss prevention (DLP) rules where possible to flag unauthorized exfiltration attempts.

Apply Least Privilege Principles: Limit user accounts so that routine activity does not run with elevated privileges. Preventing unnecessary admin rights reduces the impact of persistence mechanisms and malware installation.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0010 Exfiltration	TA0006 Credential Access
TA0005 Defense Evasion	TA0003 Persistence	TA0009 Collection	T1041 Exfiltration Over C2 Channel
T1583.001 Domains	T1583 Acquire Infrastructure	T1189 Drive-by Compromise	T1204 User Execution
T1027.010 Command Obfuscation	T1027 Obfuscated Files or Information	T1105 Ingress Tool Transfer	T1059.002 AppleScript
T1059 Command and Scripting Interpreter	T1555 Credentials from Password Stores	T1555.001 Keychain	T1005 Data from Local System

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	231c4bf14c4145be77aa4fef36c208891d818983c520ba067dda62d3bbbf547f, eb7ede285aba687661ad13f22f8555aab186debbadf2c116251cb269e913ef68, 4549e2599de3011973fde61052a55e5cdb770348876abc82de14c2d99575790f, b01c13969075974f555c8c88023f9abf891f72865ce07efbcee6c2d906d410d,5 a4e47fd76dc8ed8e147ea81765edc32ed1e11cff27d138266e3770c7cf953322, 95b97a5da68fcb73c98cd9311c56747545db5260122ddf6fae7b152d3d802877
Domains	mac-safer[.]com, rescue-mac[.]com

TYPE	VALUE
URLs	hxxps[:]//icloudservers[.]com/gm/install[.]sh, hxxps[:]//macostutorial[.]com/iterm2/install[.]sh, hxxps[:]//icloudservers[.]com/gm/update, hxxps[:]//macostutorial[.]com/iterm2/update, hxxps[:]//github[.]com/jeryrymoore/Iterm2

References

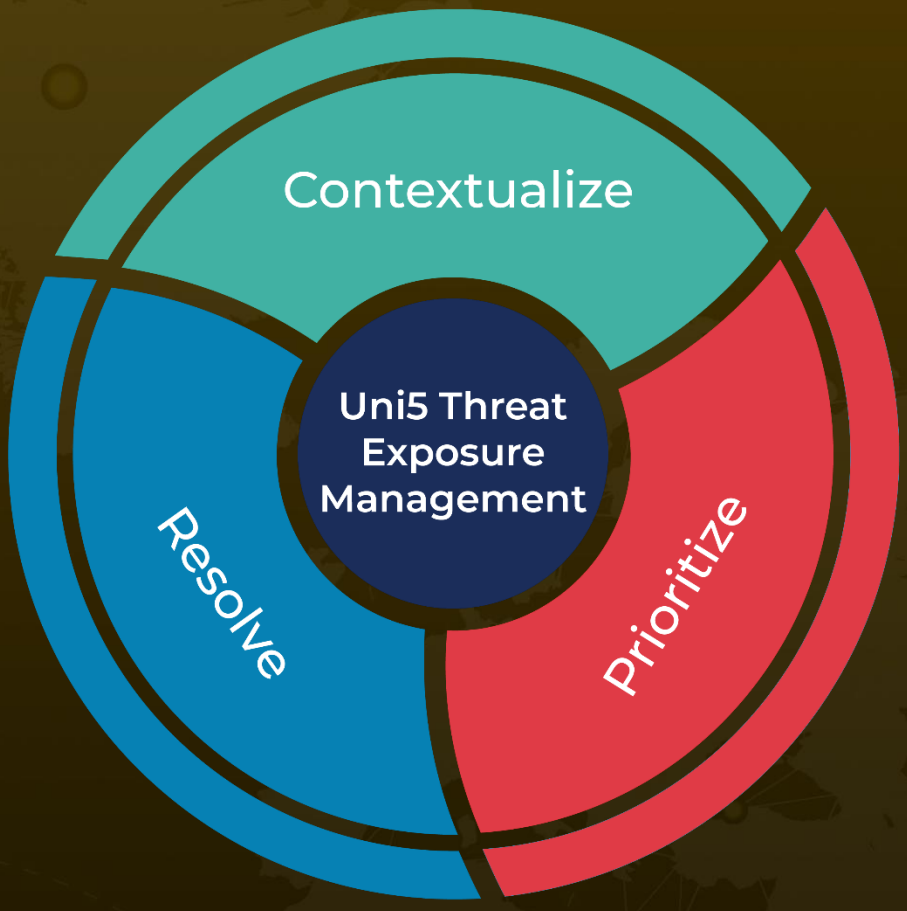
https://www.crowdstrike.com/en-us/blog/falcon-prevents-cookie-spider-shamos-delivery-macos/

https://www.hivepro.com/new-atomic-stealer-macos-malware-steals-browser-cookies-and-cryptocurrency-wallets/

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

August 26, 2025 • 4:30 AM

More at www.hivepro.com