Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

GlassWorm's Quiet Infiltration of Mac Systems

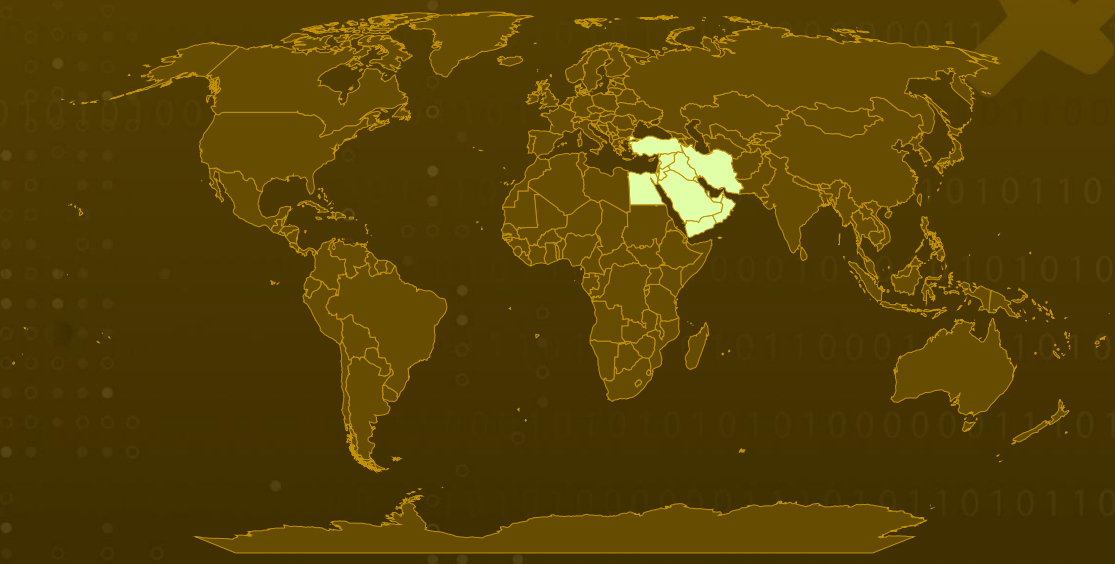
Date of Publication	Last Update Date	Admiralty Code	TA Number
January 2, 2026	March 19, 2026	A1	TA2026001

Summary

First Seen: October 17, 2025
Malware: GlassWorm
Campaign: ForceMemo
Affected Platform: macOS
Targeted Region: Middle East
Targeted Industry: Government
Attack: GlassWorm is a stealthy malware campaign targeting macOS by exploiting malicious VS Code extensions that conceal harmful code using invisible Unicode characters. Disguised as legitimate tools, these extensions deliver trojanized cryptocurrency wallet software, quietly stealing developer credentials and digital assets.

Attack Timeline

Attack Regions



Attack Details

#1 GlassWorm is a self-propagating malware campaign that weaponizes the VS Code extension ecosystem. It conceals malicious logic using invisible Unicode characters and distributes trojanized extensions through VSCode and OpenVSX, with a current focus on macOS developers. Once installed, these extensions masquerade as legitimate tools while covertly deploying compromised cryptocurrency wallet applications.

#2 After a deliberate 15-minute delay designed to evade sandbox analysis, the malware activates. An AES-256-CBC–encrypted payload embedded in compiled JavaScript initiates credential theft targeting GitHub, npm, and OpenVSX accounts, alongside wallet data harvested from multiple extensions. Persistence is established through LaunchAgents and AppleScript, while remote control is enabled via VNC and a SOCKS proxy.

#3 Command-and-control traffic is routed through the Solana blockchain. GlassWorm actively searches for hardware wallet applications such as Ledger Live and Trezor Suite, replacing them with trojanized counterparts. This allows attackers to falsify receiving addresses, alter transaction data, capture seed phrases, and intercept device communications, effectively undermining hardware wallet security despite their air-gapped design.

Recommendations

Immediate Extension Removal: Identify and uninstall all suspected malicious extensions without delay. Treat any unverified or sideloaded extension as potentially compromised until proven otherwise.

Account and Credential Reset: Rotate all developer credentials exposed on affected machines, including GitHub access tokens, npm credentials, SSH keys, and any cached authentication material to prevent downstream compromise.

Filesystem Monitoring Controls: Implement integrity monitoring on temporary and staging directories commonly abused by malware to detect unauthorized file creation or payload execution.

Endpoint Detection Hardening: Enhance detection capabilities to flag abnormal AppleScript activity, unauthorized access to Keychain databases, and development tools initiating unexpected network connections, particularly to blockchain-based endpoints.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1195 Supply Chain Compromise	T1059 Command and Scripting Interpreter
T1547 Boot or Logon Autostart Execution	T1027 Obfuscated Files or Information	T1497 Virtualization/Sandbox Evasion	T1555 Credentials from Password Stores

T1539 Steal Web Session Cookie	**T1552** Unsecured Credentials	**T1119** Automated Collection	**T1102** Web Service
T1071 Application Layer Protocol	**T1041** Exfiltration Over C2 Channel	**T1565** Data Manipulation	**T1195.002** Compromise Software Supply Chain
T1059.002 AppleScript	**T1059.007** JavaScript	**T1027.013** Encrypted/Encoded File	**T1497.003** Time-Based Evasion
T1555.001 Keychain	**T1552.001** Credentials In Files	**T1102.002** Bidirectional Communication	**T1071.001** Web Protocols
T1565.001 Stored Data Manipulation	**T1546** Event Triggered Execution	**T1614** System Location Discovery	**T1620** Reflective Code Loading

Indicators of Compromise (IOCs)

TYPE	VALUE
Extension ID	studio-velte-distributor.pro-svelte-extension, cudra-production.vsce-prettier-pro, Puccin-development.full-access-catppuccin-pro-extension, codejoy.codejoy-vscode-extension@1.8.3, codejoy.codejoy-vscode-extension@1.8.4, l-igh-t.vscode-theme-seti-folder@1.2.3, kleinesfilmroellchen.serenity-dsl-syntaxhighlight@0.3.2, JScearcy.rust-doc-viewer@4.2.1, SIRILMP.dark-theme-sm@3.11.4, CodeInKlingon.git-worktree-menu@1.0.9, CodeInKlingon.git-worktree-menu@1.0.91, ginfuru.better-nunjucks@0.3.2, ellacrity.recoil@0.7.4, grrrck.positron-plus-1-e@0.0.71, jeronimoekerdt.color-picker-universal@2.8.91, srcery-colors.srcery-colors@0.3.9, sissel.shopify-liquid@4.0.1, TretinV3.forts-api-extention@0.3.1, cline-ai-main.cline-ai-agent@3.1.3

TYPE	VALUE
Domains	api[.]mainnet-beta[.]solana[.]com, solana-mainnet[.]gateway[.]tatum[.]io, go[.]getblock[.]us, solana-rpc[.]publicnode[.]com, api[.]blockeden[.]xyz, solana[.]drpc[.]org, solana[.]leorpc[.]com, solana[.]api[.]onfinality[.]io, solana[.]api[.]pocket[.]network
Solana C2 wallet	BjVeAjPrSKFiingBn4vZvghsGj9KCE8AJVtbc9S8o8SC, 28PKnu7RzizxBzFPoLp69HLXp9bJL3JFtT2s5QzHsEA2
IPv4	45[.]32[.]151[.]157, 45[.]32[.]150[.]251, 217[.]69[.]11[.]60, 45[.]32[.]150[.]97, 217[.]69[.]11[.]57, 217[.]69[.]11[.]99, 217[.]69[.]0[.]159, 45[.]76[.]44[.]240
URLs	hxxps[:]//calendar[.]app[.]google/M2ZCvM8ULL56PD1d6, hxxp[:]//217[.]69[.]3[.]218/qQD%2FJoi3WCWSk8ggGHiTdg%3D%3D, hxxp[:]//217[.]69[.]3[.]218/get_arhive_npm/, hxxp[:]//217[.]69[.]3[.]218/get_zombi_payload/qQD%2FJoi3WCWSk8ggGHiTdg%3D%3D

References

https://www.koi.ai/blog/glassworm-goes-mac-fresh-infrastructure-new-tricks

https://www.koi.ai/blog/glassworm-first-self-propagating-worm-using-invisible-code-hits-openvsx-marketplace

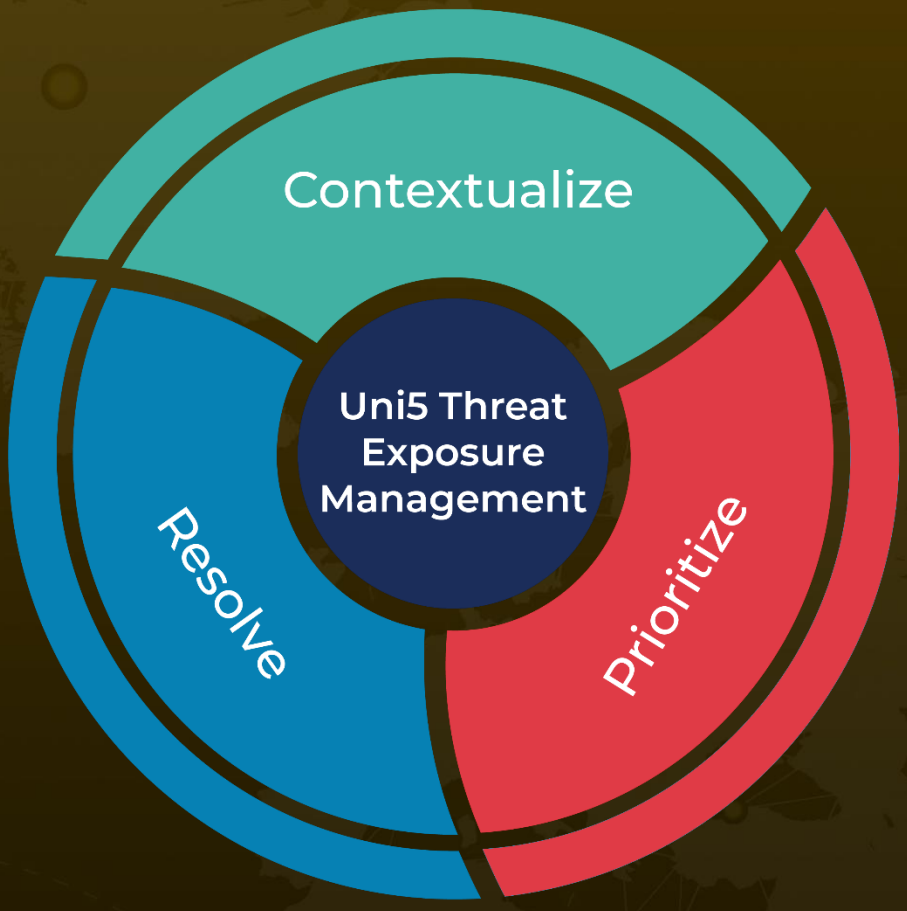
https://www.stepsecurity.io/blog/malicious-npm-releases-found-in-popular-react-native-packages---130k-monthly-downloads-compromised#indicators-of-compromise

https://www.stepsecurity.io/blog/forcememo-hundreds-of-github-python-repos-compromised-via-account-takeover-and-force-push

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

January 2, 2026 • 8:00 AM

More at www.hivepro.com