Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

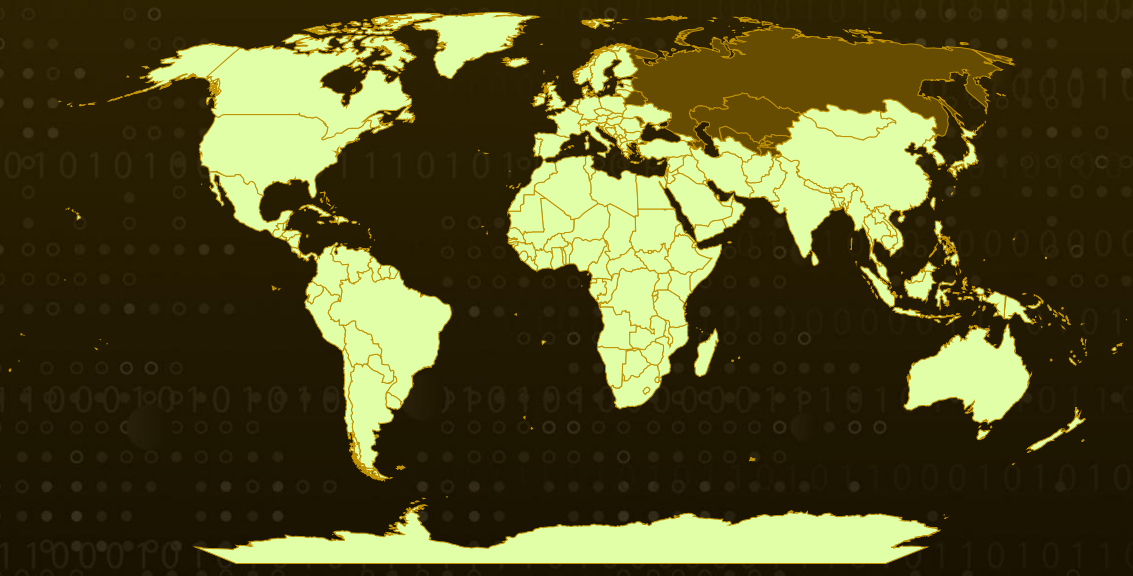
SHub Reaper A macOS Stealer Wearing Three Trusted Masks

Date of Publication	Admiralty Code	TA Number
May 25, 2026	A1	TA2026143

Summary

First Seen: 2026
Targeted Regions: Global, excluding the Commonwealth of Independent States (CIS)
Targeted Platform: macOS
Targeted Products: WeChat, Miro, Apple XProtectRemediator branding, Google Software Update (impersonated); Chrome, Firefox, Brave, Edge, Opera, Vivaldi, Arc, Orion browsers; 1Password, Bitwarden, LastPass password managers; MetaMask and Phantom browser-extension wallets; Exodus, Atomic Wallet, Ledger Wallet, Ledger Live, Electrum, and Trezor Suite desktop wallets; macOS Keychain, iCloud account data, and Telegram session data
Malware: SHub Reaper
Attack: SHub Reaper is a newly identified macOS infostealer that chains together three trusted brands in a single attack. Victims are lured through fake WeChat and Miro installers, prompted to execute what appears to be a legitimate Apple security update, and then quietly stripped of browser credentials, Keychain data, and cryptocurrency wallets. The malware establishes persistence through a LaunchAgent disguised as a Google Software Update component, granting operators an enduring backdoor for remote code execution on the compromised host.

Attack Regions



Attack Details

#1

A new variant of the "SHub" macOS infostealer uses AppleScript to show a fake security update message and installs a backdoor. Dubbed Reaper, the new version steals sensitive browser data, collects documents and files that may contain financial details, and hijacks crypto wallet apps. The attack begins on fake installer pages that impersonate WeChat and Miro download sites, hosted on misspelled domains designed to look like Microsoft and other trusted brands. Before any malware is served, the page silently profiles the visitor capturing their IP address, location, graphics fingerprint, and any signs of a virtual machine or VPN and quietly checks the browser for installed password managers and cryptocurrency wallet extensions. The page blocks developer tools, traps debugging keystrokes, and replaces the screen with a Russian "Access Denied" message if it suspects analysis. The collected data is then sent to the attackers through a Telegram bot.

#2

When the visitor appears to be a viable target, Reaper sidesteps Apple's recent fix for the older "paste into Terminal" attack by launching the macOS Script Editor with a malicious script already loaded. The script is padded with ASCII art and fake installer text so the harmful command sits hidden well below what the user can see. Clicking "Run" displays a convincing "Downloading Apple Security Update" message while a hidden command quietly fetches and executes the next stage. Before continuing, the malware checks the system's language settings for Russian if it finds one, it reports back and exits. Otherwise, it pulls down the main stealer script from its command server and runs it entirely in memory, leaving nothing on disk.

#3

Reaper then displays a fake macOS password prompt to capture the user's login credentials, which it uses to unlock saved secrets on the system, followed by a harmless-looking error message to disarm suspicion. From there, it harvests data from every major browser Chrome, Firefox, Brave, Edge, Opera, Vivaldi, Arc, and Orion along with the macOS Keychain, iCloud account data, Telegram session data, and stored cryptocurrency wallets including Exodus, Atomic Wallet, Ledger Live, Electrum, and Trezor Suite. A new document-stealing module, modelled on the well-known Atomic macOS Stealer (AMOS), also sweeps the Desktop and Documents folders for business and financial files up to a total of 150 MB. Larger collections are automatically split into smaller archives and uploaded one chunk at a time to the attacker's server.

#4

After the initial theft, Reaper attempts to compromise installed cryptocurrency wallets by replacing their core application files with tampered copies pulled from the attacker's server, allowing the operators to intercept future transactions. To stay on the system, the malware disguises itself as a Google software update component and registers a background task that runs every 60 seconds. This task acts as a beacon, regularly contacting the attacker's server and, when instructed, downloading and executing new commands with the user's privileges effectively giving the attackers a persistent backdoor that survives reboots.

Recommendations

Monitor for Suspicious AppleScript and osascript Activity: Alert on `osascript` and Script Editor processes that spawn `curl`, `zsh`, or `sh` child processes; on Script Editor execution within seconds of browser activity; and on AppleScript invocations that read `com.apple.HIToolbox.plist` or write to `/tmp/shub_ ` paths.

Detect Staging and Chunked Exfiltration: Build EDR detections for newly created directories matching `/tmp/shub_ `, the helper script `/tmp/shub_split.sh`, and ZIP archives matching `/tmp/shub_mzip_ .zip`, especially when followed by outbound `curl` requests to unfamiliar HTTPS endpoints.

Detect Wallet `app.asar` Tampering: File-integrity-monitor the `app.asar` files inside Exodus, Atomic Wallet, Ledger Live, Ledger Wallet, Electrum, and Trezor Suite installations. Trigger on `xattr -cr` invocations against application bundles and on `codesign` operations that produce ad hoc signatures on wallet binaries.

Enforce Application Allow-Listing and Strict Code-Signing Verification: Use tools such as Apple's Endpoint Security framework, third-party EDR, or Santa to allow-list approved applications and to alert on the execution of ad hoc-signed or unsigned binaries, particularly when those binaries are written into application bundles such as the modified `app.asar` files Reaper uses for wallet hijacking.

Inspect for Anti-Analysis Web Fingerprinting: Tune web proxy and browser-isolation telemetry to flag pages performing WebGL fingerprinting, VM/VPN detection, browser-extension enumeration, and continuous-debugger loops, as these behaviors precede Reaper payload delivery and are common across the broader SHub family.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
Initial Access	T1189: Drive-by Compromise	
Execution	T1059: Command and Scripting Interpreter	T1059.002: AppleScript
		T1059.004: Unix Shell
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1543: Create or Modify System Process	T1543.001: Launch Agent
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
	T1140: Deobfuscate/Decode Files or Information	
	T1553: Subvert Trust Controls	T1553.001: Gatekeeper Bypass
		T1553.002: Code Signing
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1622: Debugger Evasion	
Credential Access	T1056: Input Capture	T1056.002: GUI Input Capture
	T1555: Credentials from Password Stores	T1555.001: Keychain
		T1555.003: Credentials from Web Browsers
		T1555.005: Password Managers

Tactic	Technique	Sub-technique
Discovery	T1083: File and Directory Discovery	
	T1217: Browser Information Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery
Collection	T1005: Data from Local System	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1074: Data Staged	T1074.001: Local Data Staging
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1567: Exfiltration Over Web Service	
Impact	T1565: Data Manipulation	T1565.001: Stored Data Manipulation

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	hebsbsbzjsjshduxbs[.]xyz, qq-0732gwh22[.]com, mlcrosoft[.]co[.]com, mlroweb[.]com
URLs	hxxps[:]//hebsbsbzjsjshduxbs[.]xyz/api/debug/event, hxxps[:]//hebsbsbzjsjshduxbs[.]xyz/api/bot/heartbeat, hxxps[:]//hebsbsbzjsjshduxbs[.]xyz/gate, hxxps[:]//hebsbsbzjsjshduxbs[.]xyz/gate/chunk

TYPE	VALUE
File Path	~/Library/Application Support/Google/GoogleUpdate.app/Contents/MacOS/GoogleUpdate, ~/Library/LaunchAgents/com.google.keystone.agent.plist, /tmp/shub_log.zip, /tmp/shub_split.sh, /tmp/shub_mzip_*.zip, /tmp/.c.sh, /tmp/*_asar.zip

References

https://www.sentinelone.com/blog/shub-reaper-macos-stealer-spoofs-apple-google-and-microsoft-in-a-single-attack-chain/

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 Demo of **HivePro**.

REPORT GENERATED ON

May 25, 2026 • 4:00 AM

More at www.hivepro.com