Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

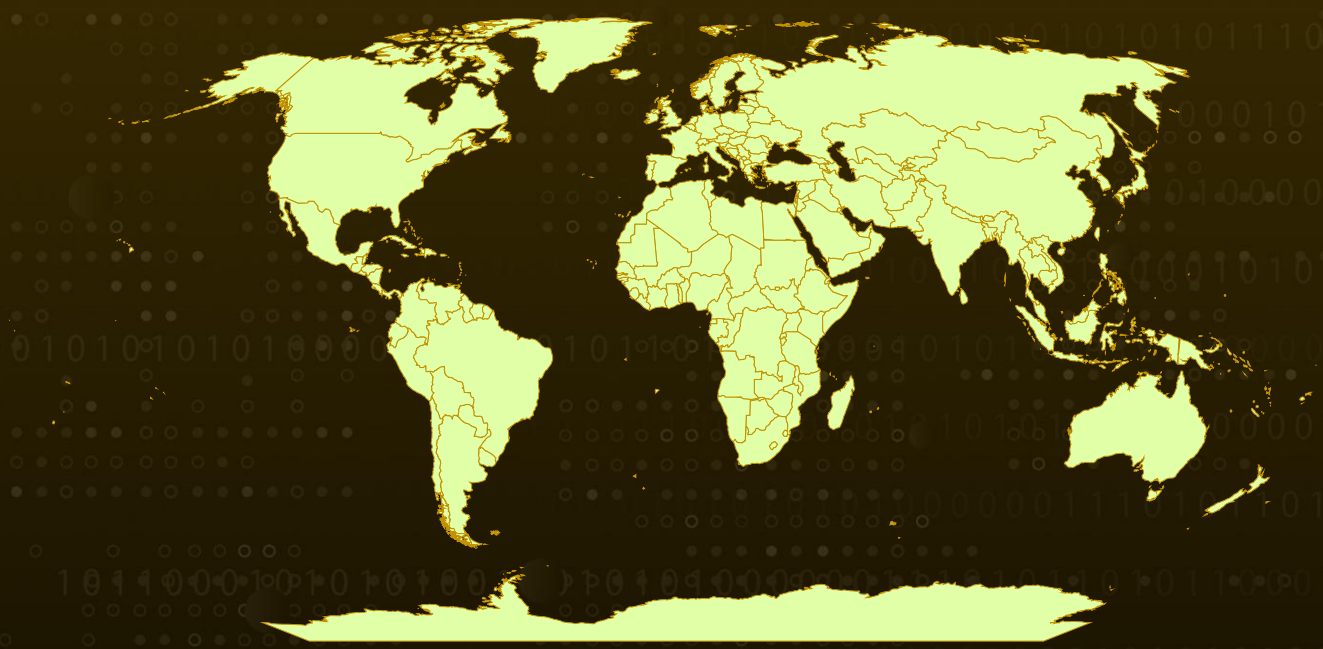
Signed, Sealed, Stolen: CrashStealer Slips Past Gatekeeper

Date of Publication	Admiralty Code	TA Number
July 14, 2026	A1	TA2026198

Summary

First Seen: May 2026
Targeted Regions: Worldwide
Targeted Platform: macOS
Malware: CrashStealer
Attack: CrashStealer is a newly identified macOS information stealer that disguises itself as Apple's legitimate CrashReporter utility to slip past both users and security tooling. It reaches victims through a signed, Apple-notarized dropper served from a fake software site, letting it clear Gatekeeper without warnings. Once running, it shows a fake password prompt, validates the entered credential locally, unlocks the login keychain, and harvests browser logins, cryptocurrency wallet extensions, password-manager vaults, and user files. The stolen data is encrypted client-side with AES-256-GCM, zipped, and exfiltrated to an attacker-controlled server over libcurl.

Attack Regions



Attack Details

#1

CrashStealer is a newly surfaced macOS information stealer that poses as Apple's crash-reporting utility to make off with credentials, keychain secrets, and cryptocurrency wallets. Its infection begins on a polished fake software site tied to the domain werkbit[.]io, which was registered in late June 2026. The download is deliberately gated behind a meeting PIN, so the malicious installer is served only to visitors who arrive with the correct code, keeping the operation low-profile and out of reach of casual scanning. The first-stage payload arrives as a signed, Apple-notarized disk image ("Werkbit Setup," delivered as Werkbit.app) carrying a valid developer ID, "Emil Grigorov (WWB7JA7AQV)." Because both the disk image and its binary are notarized, they clear macOS Gatekeeper without any warning. After the image mounts, the installer nudges the victim into running it by presenting a setup screen that instructs them to right-click the app and choose "Open."

#2

Once launched, the embedded "veltod" executable reaches out to a GitHub repository (github.com/mgothiclove) and pulls down a file named "sys.cache." That file yields a curl command used to fetch a shell script, which in turn stages the next payload, "CrashReporter.dmg," into the /tmp directory. The final binary masquerades as Apple's CrashReporter.app, borrowing the genuine tool's name, icon, and metadata. It establishes persistence by installing a LaunchAgent called com.apple.crashreporter.helper, then copies and re-signs itself; re-signing rewrites the code-signature data so the file's hash changes while the underlying code stays identical, defeating simple hash-based detection. Throughout, the malware resists analysis with control-flow flattening, encrypted strings, and layered anti-debugging, and it enumerates installed security and analysis tooling before doing anything noisy.

#3

To reach the keychain, CrashStealer presents a fake macOS password prompt framed as a routine system authorization requiring administrator privileges. When the victim types their password, the malware validates it locally using dscl, the Directory Service command-line tool, and re-prompts on failure to ensure it captures a working credential. With a valid password in hand, it unlocks the login keychain and begins collecting broadly: credentials and cookies from Chromium-family browsers and Firefox, roughly 80 cryptocurrency wallet extensions, 14 password managers, and files from the user's Documents and Downloads folders, while intentionally skipping large media files, installers, and system directories to stay lean.

#4 Before anything leaves the host, CrashStealer encrypts the collected data client-side using AES-256-GCM, an unusually strong choice for a commodity-style stealer, and packages it into hidden ZIP archives. It then uploads the compressed bundle to its command-and-control server at 179[.]43[.]166[.]242 using libcurl. The discovery of additional domains and shared backend infrastructure tied to the same operation suggests CrashStealer is one component of a larger, multi-platform campaign rather than a standalone tool.

Recommendations

Block CrashStealer Infrastructure: Immediately block the known delivery domain (werkbit[.]io), the GitHub staging path (github.com/mgothiclove), and the C2 IP address (179[.]43[.]166[.]242) at your DNS, web proxy, and firewall layers.

Hunt for the Malicious LaunchAgent: Search macOS endpoints for a LaunchAgent named com.apple.crashreporter.helper and for any CrashReporter.app running outside its legitimate system location; the genuine Apple CrashReporter does not install itself as a user LaunchAgent.

Reset Exposed Credentials and Keychain Secrets: On any host that ran the dropper, assume browser logins, keychain items (Safari logins, Wi-Fi and app passwords, private keys, certificates, and tokens), password-manager vaults, and crypto wallets are compromised; rotate passwords, revoke tokens, and move wallet funds using a separate, clean device.

Scrutinize "Right-Click to Open" Prompts: Coach users to be suspicious of any installer that tells them to bypass macOS security by right-clicking and selecting "Open," and of unexpected password prompts raised by apps such as a supposed crash reporter.

Restrict Software to Trusted Sources: Enforce installation only from the App Store or vetted internal repositories, and be wary of niche software sites that gate their downloads behind codes or PINs.

Prioritize Behavior-Based macOS Detection: Because the malware re-signs itself to change its hash, lean on behavioral detections (LaunchAgent creation, dscl password validation, keychain access, bulk browser and wallet file reads, and libcurl-based exfiltration) rather than static hash matching alone.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Persistence	T1543: Create or Modify System Process	T1543.001: Launch Agent
Defense Evasion	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1027: Obfuscated Files or Information	
	T1622: Debugger Evasion	
	T1140: Deobfuscate/Decode Files or Information	
Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
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
Collection	T1005: Data from Local System	
	T1560: Archive Collected Data	
Command and Control	T1102: Web Service	T1102.001: Dead Drop Resolver
	T1105: Ingress Tool Transfer	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	werkbit[.]io, cohezo[.]io, cohezo[.]com, cordinex[.]io, synerix[.]app, collabox[.]uk, werknova[.]co
IPv4	179[.]43[.]166[.]242
Filenames	Werkbit.app, veltod, sys.cache, CrashReporter.dmg, CrashReporter.app, com.apple.crashreporter.helper
URLs	hxxps[:]//github[.]com/mgothiclove, hxxps[:]//github[.]com/mgothiclove/pkeys/blob/main/sys[.]cache, hxxps[:]//raw[.]githubusercontent[.]com/mgothiclove/pkeys/main/sys[.]cache, hxxps[:]//endpoint-api-v1[.]com/d/f1b24e, hxxp[:]//endpoint-api-v1[.]com/d/f1b24e/download, hxxps[:]//icky-lyrical[.]com, hxxps[:]//icky-lyrical[.]com/api/download?access_code=<redacted>&type=werkbit&os=Mac, hxxps[:]//icky-lyrical[.]com/storage/secure/werkbit/mac, hxxps[:]//icky-lyrical[.]com/storage/secure/Cohezo/windows/small/69cf7d0ea7cfd/cohezo_setup[.]msi, hxxps[:]//cohezo[.]io/download?invite=OX-3SEY-64KI, hxxps[:]//cordinex[.]io/download?invite=MZ-AB95-QD50, hxxps[:]//cohezo[.]com/calendar/0f4df3a7-5914-4245-a616-311ca554ee0c, hxxps[:]//collabox[.]uk/calendar/1cdf0e32-9ba0-4be5-8823-39a2e6364a20, hxxps[:]//synerix[.]app/calendar/144f20fc-c7fb-4e58-9544-75fe9099b61c, hxxps[:]//synerix[.]app/calendar/a711f30b-b9bc-4f31-9c8e-869e7c1b2c1f, hxxps[:]//werknova[.]co/calendar/90f99c64-9fcc-451c-bae1-0b095c04e5c8

TYPE	VALUE
SHA256	3a9d703ba7f7564399365db7ab8b04238806ef7a53df0b6822f32b80bf0f5a80, 88334ea00ff94a366cd2a9283a508b97c269839894fddfe91913f3d92e95b6ab, f3857c0b84a24b7fc912d55f8b14c67c23d5837b1a6932164d5d62273d4affeb, a1966a6d6f54a025f30d55571d21d6537977ca73ffa734c13494b9c806cd7007, 5bb675af9c403896d5f31611cf42304cf482d16f6f3ab6a868a9aa853aa5c179, 08801f81960cd8c1077b4aa2e8124840d56a272842fdcc73263c9968e787e0bd, 09bd60ce11ee4324e2052a439a08676e31aac787edda3f9bd02325390b5db2d2, 4ed199e27a4dc193468569b221b19180e5ae95cab8df84d92e082b68d33672f5, 81ef05cc4d07cd22cd7cd7099f278dd9b9a3ae8ad4770b3d387892e1c6cfb7d7, fba5bbe87fa351eedf2f3c16653cc9e4196d73604529bb50a609e2d3ebf1828b
File Paths	/private/tmp/.CrashReporter/CrashReporter.app/Contents/MacOS/CrashReporter, ~/Library/Caches/com.apple.crashreporter/CrashReporter.app, ~/Library/LaunchAgents/com.apple.crashreporter.helper.plist, ~/.cache/com.apple.crashreporter/, ~/.cache/com.apple.crashreporter/.zx_<8-hex>.zip, ~/.cache/com.apple.crashreporter/.brw_<random>/Keychain/login.keychain-db, ~/.cache/com.apple.crashreporter/.brw_<random>/password.txt, ~/.cache/.sys_auth, /private/tmp/agent_crash_marker

References

https://www.jamf.com/blog/crashstealer-macos-infostealer-analysis/

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

July 14, 2026 • 08:30 AM

More at www.hivepro.com