Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

MacSync A Notarized macOS Malware That Slips Past Gatekeeper

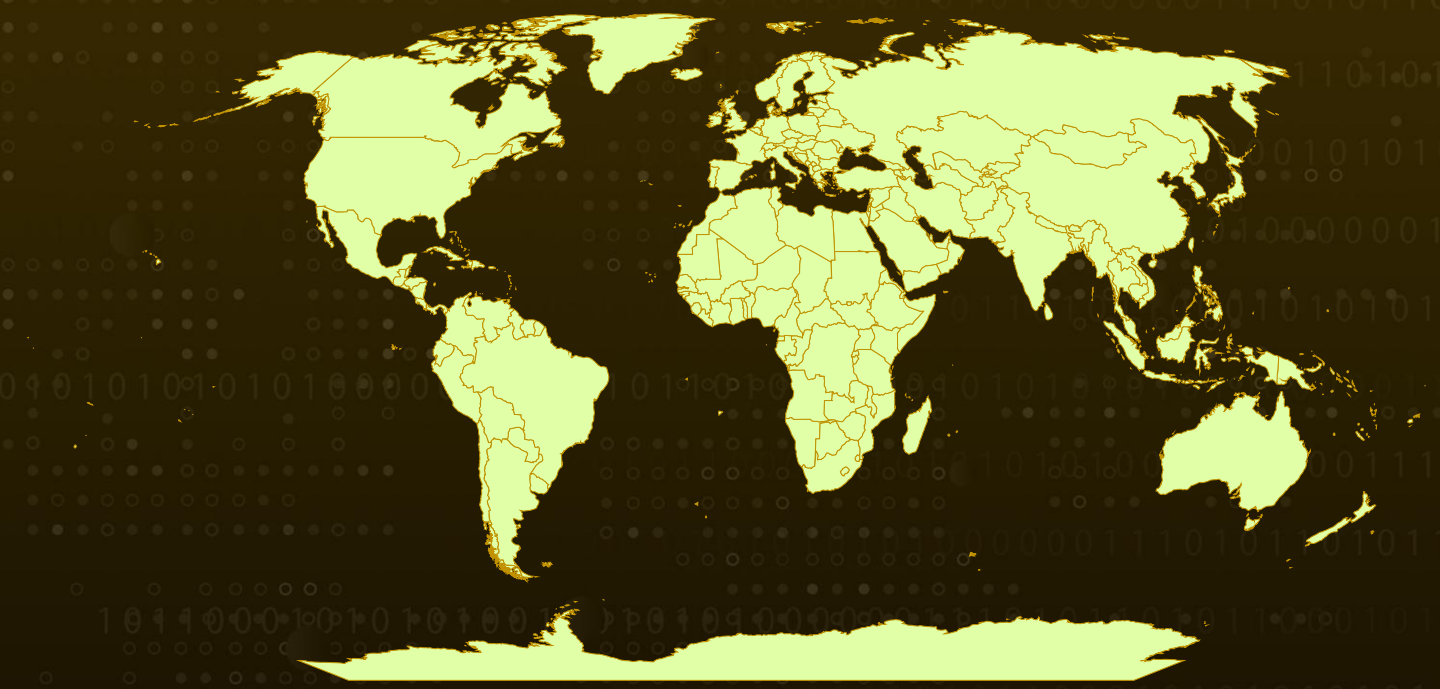
Date of Publication	Admiralty Code	TA Number
December 26, 2025	A1	TA2025390

Summary

First Seen: 2025
Malware: MacSync Stealer
Affected OS: macOS
Targeted Region: Worldwide

Attack: MacSync Stealer is an advanced macOS information-stealing malware that abuses Apple's code-signing and notarization processes to bypass Gatekeeper protections without user interaction. By leveraging trusted digital signatures, decoy files, and execution-chain cleanup, this latest variant demonstrates a significant evolution in macOS malware delivery and underscores the growing risk posed by notarized threats targeting sensitive user and enterprise data.

Attack Regions



Attack Details

#1 MacSync Stealer represents a marked escalation in macOS malware sophistication. It is delivered as a fully code-signed and notarized Swift application capable of deploying malicious payloads without any user interaction, effectively bypassing traditional trust signals relied upon by macOS users.

#2 The latest variant masquerades as a legitimate messaging application installer distributed via the domain zkcall[.]net. Because the application carries valid digital signatures and has passed Apple's notarization process, Gatekeeper raises no warnings during installation, allowing the infection to proceed silently.

#3 Once executed, the dropper retrieves an obfuscated script from its command-and-control infrastructure. A Swift-based helper, runtimectl, orchestrates the entire infection chain: verifying internet connectivity, executing credential-harvesting routines, and exfiltrating sensitive information.

#4 To further evade detection, the malware inflates its DMG size to over 25 MB by embedding decoy PDF files, removes execution artifacts after use, and performs connectivity checks to avoid sandboxed analysis environments. The result is a stealthy, trust-abusing delivery mechanism that exploits Apple's security model rather than breaking it, highlighting a shift toward abuse of legitimate platform protections as an attack vector.

Recommendations

Strengthen Notarization Review Processes: Expand analysis of notarized applications to detect obfuscated scripts, suspicious network behavior, and abnormal bundle inflation tactics commonly used by advanced macOS malware.

Enforce Runtime Behavioral Monitoring: Deploy endpoint security solutions capable of monitoring post-installation behavior, including script execution, credential access, and unauthorized data exfiltration, rather than relying solely on pre-execution trust signals.

Monitor for Artifact Cleanup and Evasion Tactics: Detect behaviors such as script self-deletion, decoy file usage, and environment checks that indicate attempts to evade sandboxing or forensic analysis.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1059 Command and Scripting Interpreter	**T1543** Create or Modify System Process	**T1553** Subvert Trust Controls	**T1553.002** Code Signing
T1553.001 Gatekeeper Bypass	**T1027** Obfuscated Files or Information	**T1027.010** Command Obfuscation	**T1140** Deobfuscate/Decode Files or Information
T1497 Virtualization/Sandbox Evasion	**T1497.001** System Checks	**T1070** Indicator Removal	**T1070.004** File Deletion
T1036 Masquerading	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1555** Credentials from Password Stores
T1005 Data from Local System	**T1041** Exfiltration Over C2 Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
Filename	zk-call-messenger-installer-3.9.2-lts.dmg, co.runtime.helper.b3f9a2.dmg
SHA256	be961ec5b9f4cc501ed5d5b8974b730dabcdf7e279ed4a8c037c67b5b935d51a, 4ae745bc0e4631f676b3d0a05d5c74e37bdfc8da3076208b24e73e5bbea9178f, ecfaa20f25e11878686249c7094706bc3dcd2dc0ace0f2932a39d1bfdac85863, 7cfe0b119e616ac81ddb1767a5c7f40bec67d91fdd66e53490c0225789537073, 06c74829d8eee3c47e17d01c41361d314f12277d899cc9dfa789fe767c03693e, c4d3e5cdb264eded917cd61b8131c40715c0ee3f4d2c94c84d60fa295ca4ed97, 9990457feac0cd85f450e60c268ddf5789ed4ac81022b0d7c3021d7208ebccd3, 9d43e059111460c4f81351a062fb7eb7dbfd34988a06d756c7206f330c06cb42, 2e671bd9673d174de9b4ad8fd03049859e1d2d17ac9bc49ecc5d736505002937
URL	hxxps[:]//gatemadenp.]space/curl/985683bd660c0c47c6be513a2d1f0a554d52d241714bb17fb18ab0d0f8cc2dc6
Domains	focusgroovy[.]com zkcall[.]net

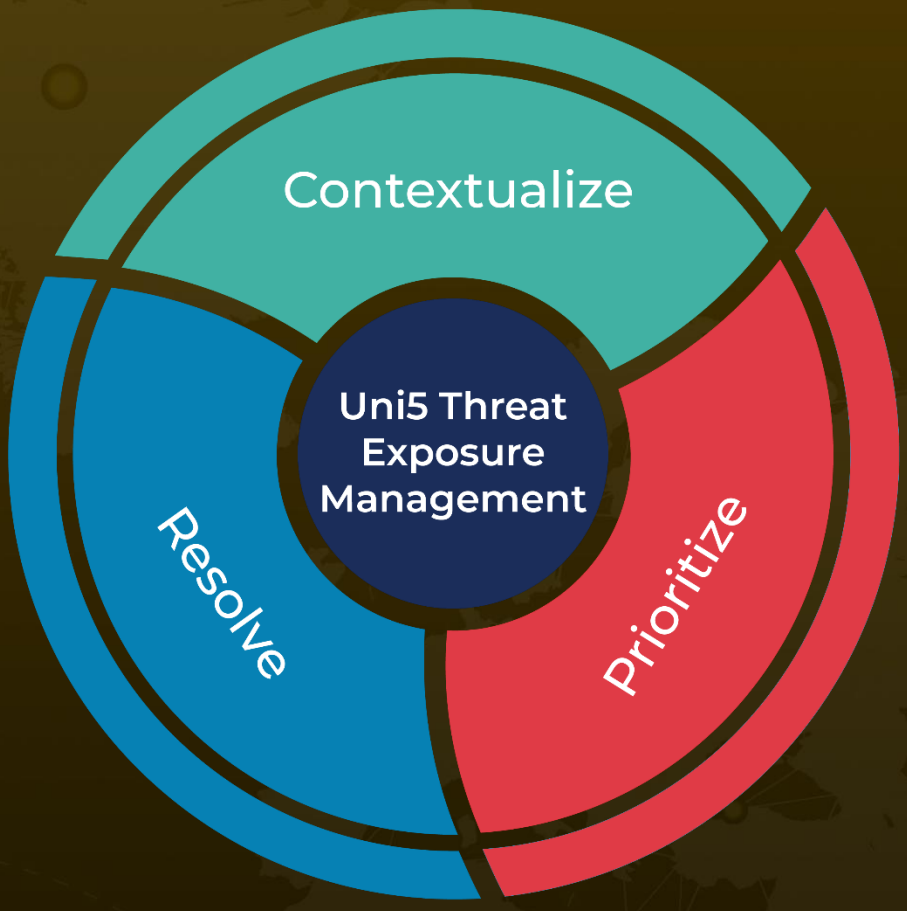
References

https://www.jamf.com/blog/macsync-stealer-evolution-code-signed-swift-malware-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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 26, 2025 • 5:30 AM

More at www.hivepro.com