Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

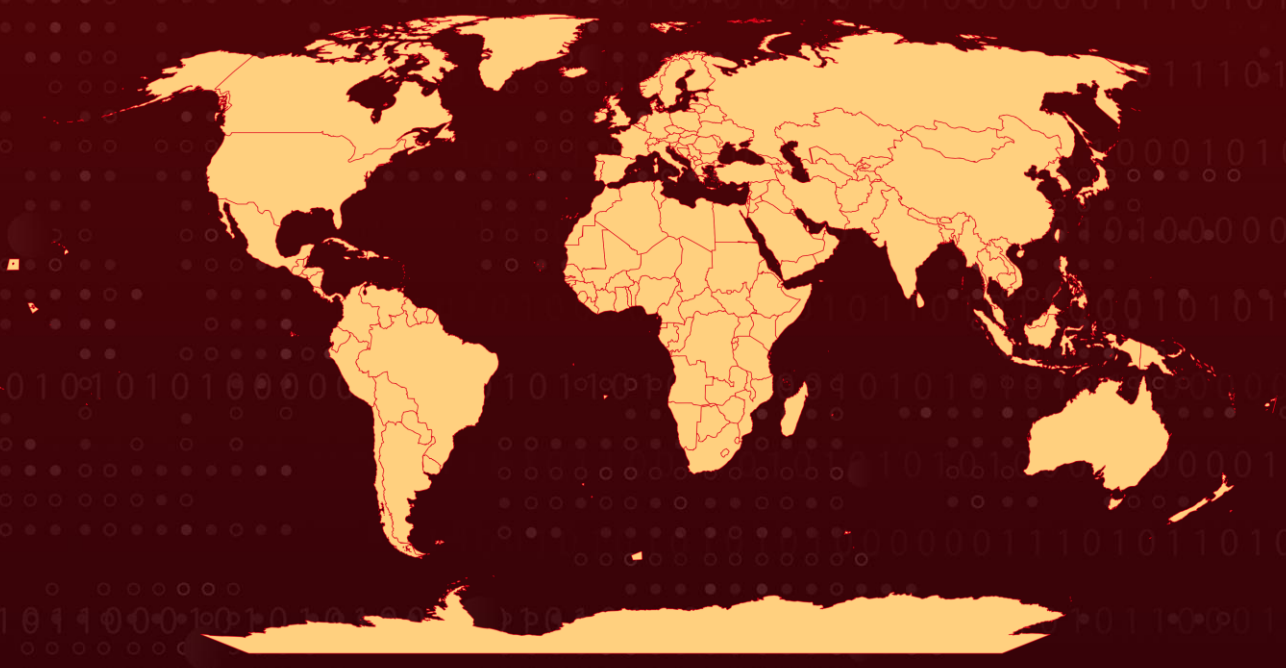
Stealer Malwares Delivered Through Malicious Ads and Bogus Websites

Date of Publication	Admiralty Code	TA Number
April 2, 2024	A1	TA2024125

Summary

First Discovered: March 2024
Attack Region: Worldwide
Malware: Atomic Stealer, Realst stealer
Attack: Two distinct stealer malware programs, including Atomic Stealer, are being distributed to Apple macOS users through deceptive advertisements and counterfeit websites. These recent attacks have successfully infected victims' macOS devices with infostealers.

Attack Regions



Attack Details

#1 In the past year, macOS has been targeted by infostealers aiming at individuals in the crypto industry, with the goal of stealing credentials and data from various wallets. These attackers have displayed a creative evolution in their tactics, as evidenced by two recent attacks deploying infostealers onto victims' systems.

#2 The first attack, involving **Atomic Stealer**, begins with the dissemination of the malware via sponsored advertisements, leading users to a deceptive website, aricl[.]net, designed to resemble the legitimate Arc web browser site. The DMG file is ad-hoc signed, and users are instructed to bypass Gatekeeper warnings by right-clicking the app. The malware employs minimal strings, mostly xor-encoded, to evade detection. It executes a function named bewta(), which de-xors bytes using the hardcoded xor key 0x91, then utilizes AppleScript payloads for information stealing, and sends the stolen data via a POST request to the attacker's server.

#3 The second attack introduces a counterfeit application named Meethub, posing as a virtual meeting platform. Perpetrators, with a notable online presence, engage victims via direct messages on social media platforms, discussing topics like podcast recordings or job prospects. A fraudulent website, meethub[.]gg, lures victims with free group meeting scheduling software but delivers a stealer malware to harvest keychain data, browser credentials, and cryptocurrency wallet information.

#4 This malware utilizes Chainbreaker, an open-source tool integrated into the application, to gather passwords from unlocked keychains, retrieve browser login data, and pilfer information from cryptocurrency wallets. Notably, similarities exist between this stealer and the previously identified **Realst stealer**, including the use of Chainbreaker, the main executable written in Rust, and usage of same Chainbreaker Mach-O hash, although a direct link between them has not been established yet.

#5 These attacks represent a broader trend of infostealer attacks targeting macOS users, particularly those involved in the crypto industry, over the past year. These attacks can yield significant profits for the perpetrators. It's crucial for individuals in the industry to stay informed about public information regarding their assets and connections. Both APT groups and cybercriminals are engaging in social engineering tactics to exploit crypto assets, highlighting the importance of remaining vigilant and alert to such threats.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Exercise caution when installing third-party apps: Stick to trusted sources and thoroughly review app permissions. Unauthorized or poorly vetted apps may gain access to your keychain data, compromising your security.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
T1140 Deobfuscate/Decode Files or Information	T1056 Input Capture	T1003 OS Credential Dumping	T1539 Steal Web Session Cookie
T1555 Credentials from Password Stores	T1566 Phishing	T1566.002 Spearphishing Link	T1204 User Execution
T1204.002 Malicious File	T1608 Stage Capabilities	T1608.001 Upload Malware	T1583 Acquire Infrastructure

T1583.006 Web Services	T1553 Subvert Trust Controls	T1553.002 Code Signing	T1560 Archive Collected Data
T1406 Obfuscated Files or Information	T1567 Exfiltration Over Web Service	T1082 System Information Discovery	T1059 Command and Scripting Interpreter
T1059.002 AppleScript			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	9d103cbad2b56f53a36f93316feda1de5513394d, ba59bb35e8dfbe77676c8130c8c2d61c22b14564, d294b86c5aa7e90ff1f7367eb9fdad8d47193f22, af33c2bc39371a5667b65c38a62919c59f5ad084, 56871908b00a1efa1d3671d0b03b8f69da6d534a, 28e35f4d92f3a0bf85fdffeb5b695119de823548, 28cc0be3aad1479c4d4ba616be6462a2c5c7ac18, 0ac59146723d72b2faad6a637cdd9fb2a6221f7e, 7f22760d6d85f8173292d39ea087f35695ad65ab, 3865636ed27ae81f146ed5b9ac9a25f53a6d10a7, 50b8af2019adbbea310bce0259b4a3f3da2e4d7d, eecf5ffc338b97602b5b8f8ab8ccc51dcb8ffd8a, 596fd483314c3cce43d8b5ed38b5202c29a60b14
URL	https[:]//aricl[.]net, https[:]//airci[.]net, https[:]//meethub[.]gg
IP	193[.]233[.]132[.]188, 46[.]101[.]104[.]172

References

https://www.jamf.com/blog/infostealers-pose-threat-to-macos/

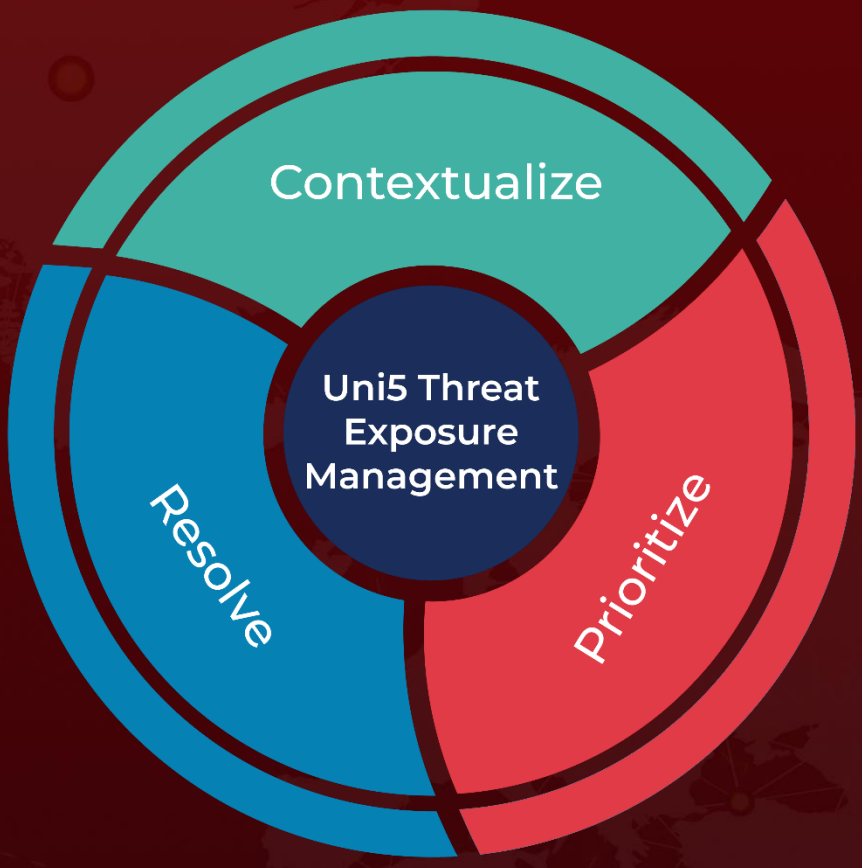
https://www.hivepro.com/threat-advisory/atomic-stealer-sneaks-in-via-fake-browser-updates/

https://www.hivepro.com/threat-advisory/realst-infostealer-hides-behind-phony-blockchain-games/

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

April 2, 2024 • 7:15 AM

More at www.hivepro.com