Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

New Atomic Stealer MacOS malware Steals Browser Cookies and Cryptocurrency Wallets

Date of Publication	Admiralty Code	TA Number
May 05, 2023	A1	TA2023212

Summary

First appeared: April, 2023
Attack Region: Worldwide
Affected Platform: MacOS
Malware: Atomic Stealer
Attack: Atomic Stealer malware is a full-featured infostealer designed to steal sensitive data from macOS users. The malware can grab account passwords, browser data, session cookies, and crypto-wallets.

Attack Regions

Attack Details

#1 A new malware called Atomic macOS Stealer (AMOS) has been discovered by Cyble Research and Intelligence Labs (CRIL) that is designed to target macOS and can steal sensitive information from the victim's machine. The malware is constantly updated and has various capabilities, including keychain extraction, crypto wallet theft, browser details stealing, file grabbing, system information collection, and command and control (C&C) server communication.

#2 It is distributed through a '.dmg' file and is a 64-bit Golang executable file that is FUD (Fully Undetectable) on Virustotal. The malware works via a one-hit smash-and-grab methodology, with no attempt to gain persistence, and instead relies on a crude but effective method of spoofing AppleScript to extract users' login passwords.

#3 The malware can target crypto wallets like Electrum, Binance, Exodus, Atomic, and Coinomi. The developer behind the malware offers additional services at a price of $1000 per month, such as a web panel for managing victims, meta mask brute-forcing for stealing seed and private keys, and crypto checker.

Recommendations

- Use official software and security tools, download and install software only from the official Apple App Store and use a reputed antivirus and internet security software package on your system.
- Protect your accounts with strong passwords and enable multi-factor authentication wherever possible to add an extra layer of security.
- Be wary of opening any links received via emails delivered to you, be careful while enabling any permissions, and keep your devices, operating systems, and applications updated to ensure they have the latest security patches and protections.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0001 Initial Access
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1007 System Service Discovery
T1204 User Execution	T1566 Phishing	T1204.002 Malicious File	T1059 Command and Scripting Interpreter
T1218 System Binary Proxy Execution	T1110 Brute Force	T1176 Browser Extensions	T1641.001 Transmitted Data Manipulation
T1555.001 Keychain	T1083 File and Directory Discovery	T1555.003 Credentials from Web Browsers	T1132 Data Encoding
T1132.001 Standard Encoding	T1041 Exfiltration Over C&C Channel	T1560 Archive Collected Data	T1641 Data Manipulation

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	5e0226adbe5d85852a6d0b1ce90b2308
URL	hxxp[:]//amos-malware[.]ru/sendlog
SHA256	15f39e53a2b4fa01f2c39ad29c7fe4c2fef6f24eff6fa46b8e77add58e7ac709
Domains	amos-malware[.]ru amos-malware[.]ru/sendlogillegal
IPV4	37[.]220.87[.]16

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	0a87b12b2d12526c8ba287f0fb0b2f7b7e23ab4a 24c9f5c90ad325dae02aa52e2b1bac2857ae2faf 36997111b5e7aa81b430a72df9f54bac2a9695ba 7534b4ef7727d14b4fdd32d18651d32572c7747b 0db22608be1172844c0ebf08d573ea4e7ef37308 2681a24f0ec0b1c153cc12d5d861c0c19c8383ea 385b9cc7d3147f049e7b42e97f242c5060fc9e97 46426409b9e65043b15ce2fcddd61213ff4e5156 48a0a7d4f0ae4b79b4f762857af3bbb02e8ab584 4f25d1a1aa18c8d85d555cd7a8f1cf2cf202af8c 58a3bddbc7c45193ecbefa22ad0496b60a29dff2 5d2e995fa5dce271ac5e364d7198842391402728 79007aabf9970e0aff7df52fd1c658b69f950c6f 793195d48cce96bb9b4fc1ee5bac03b371db75f7 82f4647e6783b012fc9a1f86108c644fcf491cf6 849cde22d1d188cc290bb527bbd7252ad07099af 9058ab6e05cb1f9ce77e4f8c18324a6827fb270d 97b19a82a32890d5ddaecac5a294cc3384309ea9 98f98a737a26c9dd1b27c474715976356ea4e18b aab3a2897950e85a2b957f77d2f100e61e29061c b42243d72765f142953bb26794b148858bff10a8 ca05f80fe44174d1089077f4b2303c436653226f d5db5a11b9605d54cf66a153b0112b91c950d88f d9d46ecfc1100d2b671ad97dc870e879d2634473 de465aad6cde9f0ce30fce0157bc18abf5a60d40 e114f643805394caece2326fb53e5d3a604a1aa9 f28025717f9db8a651f40c8326f477bf9d51a10f 1f29b00c18bc0b7e1dfee5e79f8111da09f8fab8 a02730f734032ed0f3b3705926b657aa4b88d720 c70fdf4362eb56032793ab08e6aeb892f1bd4a9b e951b889aabca7ee5b0ff9d06a057884ed788b70

References

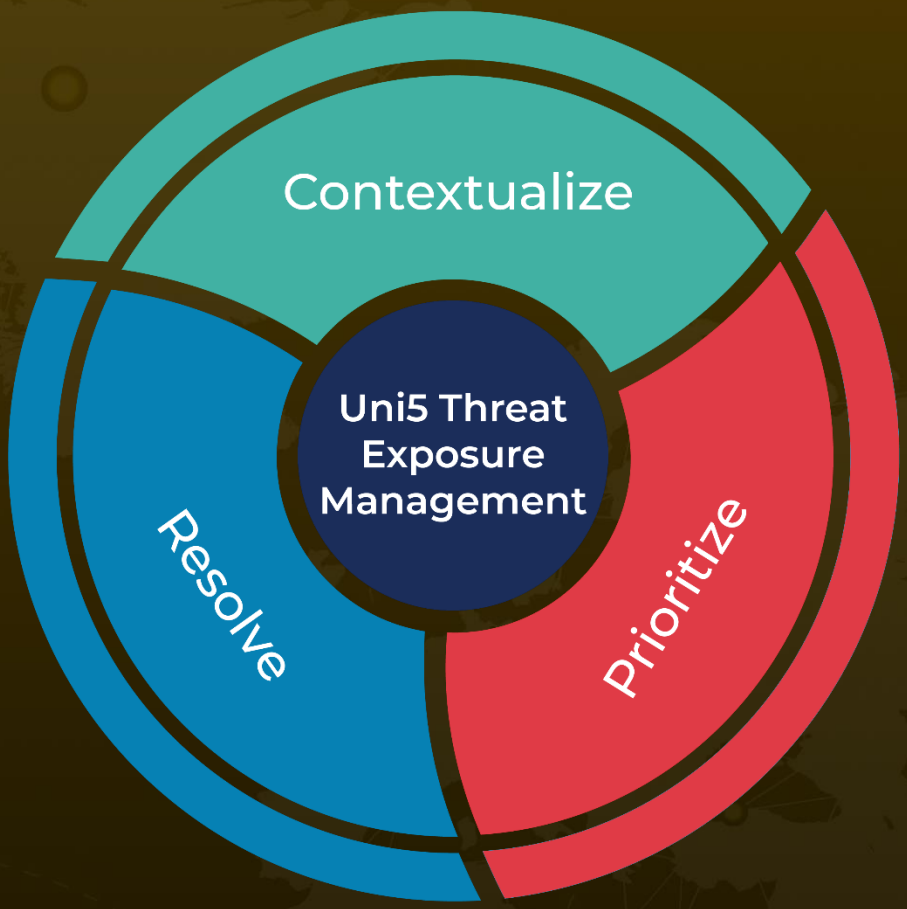
https://www.sentinelone.com/blog/atomic-stealer-threat-actor-spawns-second-variant-of-macos-malware-sold-on-telegram/

https://blog.cyble.com/2023/04/26/threat-actor-selling-new-atomic-macos-amos-stealer-on-telegram/

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

May 05, 2023 • 4:30 AM

More at www.hivepro.com