Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

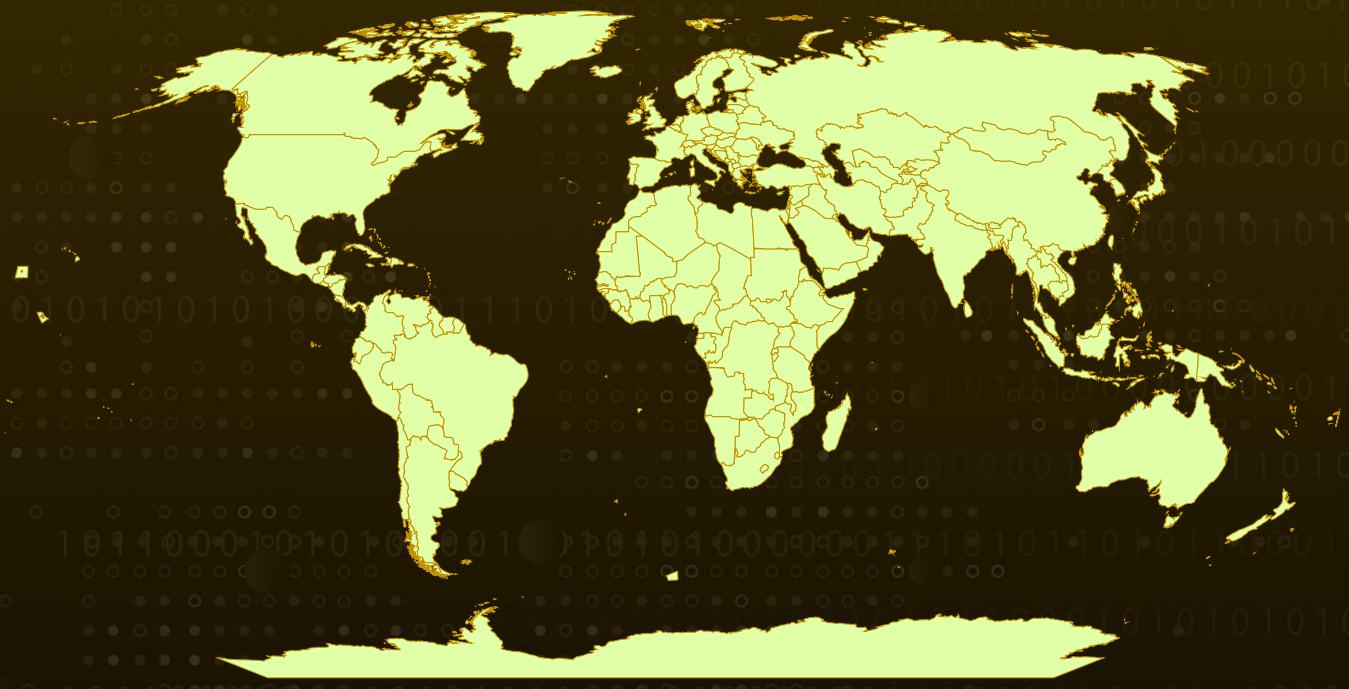
Cthulhu Stealer: The New Malware Targeting Mac Users

Date of Publication	Admiralty Code	TA Number
August 26, 2024	A1	TA2024327

Summary

First Seen: 2023
Targeted Countries: Worldwide
Malware: Cthulhu Stealer, Atomic Stealer
Affected Platform: macOS
Attack: The Cthulhu Stealer is a macOS-targeted malware written in GoLang that disguises itself as legitimate software to steal passwords and cryptocurrency wallet data. It uses osascript to prompt users for credentials, storing the stolen information in text files, and sending it to its operators. Despite operational issues among its creators, the malware highlights the growing threat of macOS-targeted attacks.

Attack Regions



Attack Details

#1

Cthulhu Stealer is a malware-as-a-service (MaaS) that targets macOS users and steals a wide range of sensitive information. Written in GoLang, a language known for its cross-platform capabilities. Cthulhu Stealer has been available since late 2023 for $500 per month, allowing multiple cybercriminals to use it against unsuspecting Mac owners.

#2

Cthulhu Stealer disguises itself as popular software like CleanMyMac, Grand Theft Auto IV, or Adobe GenP to trick users into installing it. The malware comes packaged as a disk image (DMG) file containing two binaries to target both Intel and Apple Silicon Macs. If the user tries to open the fake app, Gatekeeper warns that the software is unsigned. If the user bypasses this warning, the malware immediately asks for the user's system password, mimicking a legitimate system prompt.

#3

Once it has the necessary permissions, Cthulhu Stealer can access and steal a wide range of sensitive data, including saved passwords from iCloud Keychain, browser information, Telegram account details, and MetaMask cryptocurrency wallet credentials.

#4

Cthulhu Stealer operates by creating a directory to store the stolen data and compressing it into a zip file, which is then sent to the malware's command-and-control servers. The malware’s functionality is similar to that of Atomic Stealer, suggesting it might be a modified version of the latter.

#5

The malware is believed to be based on another macOS MaaS called Atomic Stealer, but charges affiliates half the price. The malware’s developers, known as the "Cthulhu Team," rented out their service to other criminals for a monthly fee, but faced complaints and disputes that led to their ban from malware marketplaces. This incident highlights that despite macOS's reputation for security, it is increasingly targeted by sophisticated malware.

Recommendations

Download Software from Trusted Sources: Always download applications from reputable sources, such as the Mac App Store or official developer websites. Avoid third-party sites that may host malicious versions of popular software.

Enable macOS Security Features: Use built-in features like Gatekeeper and XProtect to prevent unauthorized installations and block malware.

Keep macOS Updated: Regularly update your macOS to the latest version to ensure you have the latest security patches and features. This helps protect against vulnerabilities that malware may exploit.

Use Antivirus Software: Consider installing reputable antivirus software that can provide additional protection against malware threats. Regularly scan your system for potential threats.

Monitoring and Detection: Deploy advanced threat detection and monitoring tools capable of identifying and mitigating malware attacks in real-time. This includes behavior-based analytics, intrusion detection systems, and endpoint protection solutions.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0006 Credential Access
TA0002 Execution	TA0010 Exfiltration	TA0005 Defense Evasion	T1036 Masquerading
T1204 User Execution	T1059.002 AppleScript	T1059 Command and Scripting Interpreter	T1555 Credentials from Password Stores

T1555.001 Keychain	T1555.003 Credentials from Web Browsers	T1087 Account Discovery	T1082 System Information Discovery
T1074 Data Staged	T1005 Data from Local System	T1041 Exfiltration Over C2 Channel	T1657 Financial Theft

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	6483094f7784c424891644a85d5535688c8969666e16a194d397dc66779b0b12, 96f80fef3323e5bc0ce067cd7a93b9739174e29f786b09357125550a033b0288, de33b7fb6f3d77101f81822c58540c87bd7323896913130268b9ce24f8c61e24, e3f1e91de8af95cd56ec95737669c3512f90cecbc6696579ae2be349e30327a7, f79b7cbc653696af0dbd867c0a5d47698bcfc05f63b665ad48018d2610b7e97b
IPv4	89[.]208[.]103[.]185
MD5	897384f9a792674b969388891653bb58
URLs	hxxp://89[.]208[.]103[.]185, hxxp://89[.]208[.]103[.]185:4000/autocheckbytes, hxxp://89[.]208[.]103[.]185:4000/notification_archive

References

https://www.cadosecurity.com/blog/from-the-depths-analyzing-the-cthulhu-stealer-malware-for-macos

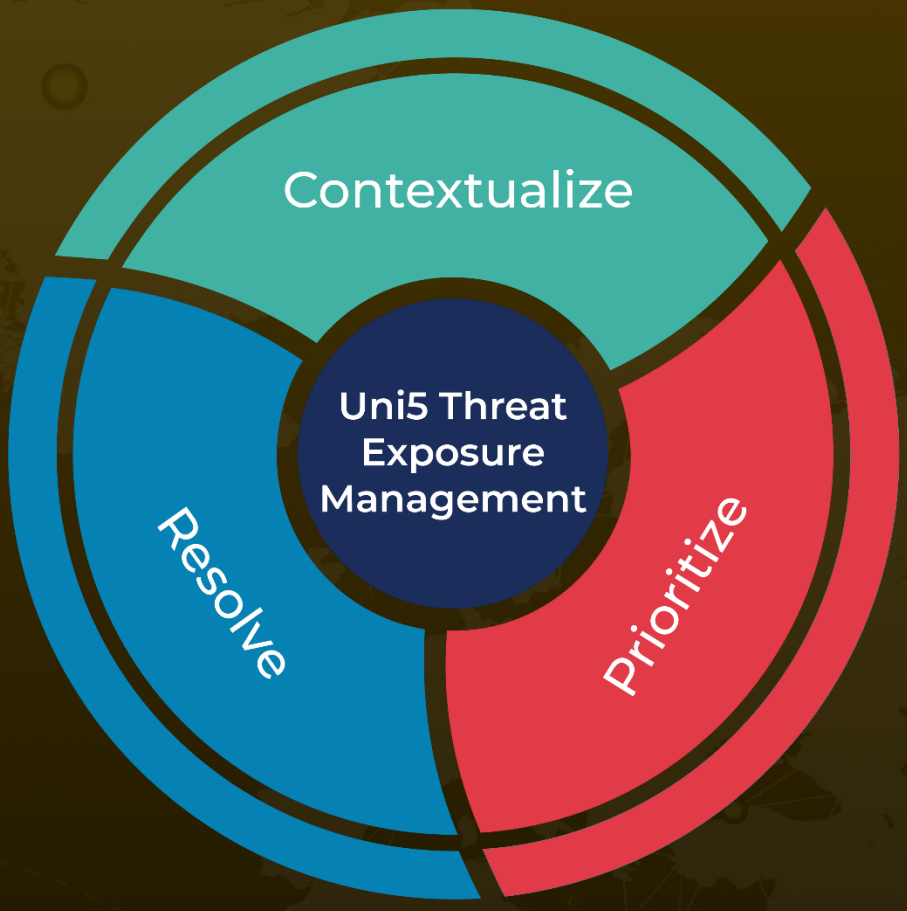
https://www.hivepro.com/new-atomic-stealer-macos-malware-steals-browser-cookies-and-cryptocurrency-wallets/

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

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

August 26, 2024 • 4:00 AM

More at www.hivepro.com