UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0295

MACSTEALER TARGETS APPLE DEVICES

DATE ISSUED: 27th March 2023

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

A new information-stealing malware targets Apple's macOS operating system to harvest sensitive and confidential information stored in the iCloud KeyChain and web browsers.

BREAKDOWN

Security researchers at Uptycs discovered a new information-stealing malware dubbed MacStealer with capabilities to steal sensitive information from compromised Apple devices. It is distributed as malware-as-a-service (MaaS), with pre-existing DMG (Disk Image) payloads that can be mounted on Apple's Catalina, Big Sur, Monterey, and Ventura operating systems. A user must click on an unsigned DMG file (weed.dmg), which will trigger the execution of a fake password prompt to grant access to the System Settings app. The malware harvests the login credentials and saves them in a ZIP file. Interestingly, this data is exfiltrated using Telegram as a command-and-control (C2) platform. MacStealer can extract information from the iCloud Keychain database, passwords, and credit card information from browsers like Google Chrome, Mozilla Firefox, and Brave. It also has features that could harvest Microsoft Office files, images, archives, and Python scripts.

REMEDIATION STEPS

- Install anti-malware software: To protect endpoints from malware, regularly update the agent to detect and block the latest threat.
- Keep software up to date: Keep operating systems, software applications, and plug-ins updated with the latest security patches.
- Use strong passwords: Use strong, complex passwords and to avoid reusing the same password across multiple accounts.
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.

REFERENCES & RESOURCES

The Bleeping Computer https://www.bleepingcomputer.com/news/security/new-macstealer-macos-malware-steals-passwords-from-icloud-keychain/