مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Cthulhu Stealer Targets macOS

Tracking #:432316185

Date:27-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new macOS malware, "Cthulhu Stealer," that is designed to steal sensitive data from Apple devices, including login credentials, cryptocurrency wallet information, and system data.

TECHNICAL DETAILS:

A new macOS malware, dubbed "Cthulhu Stealer," has emerged as a significant threat to Apple users. This information stealer, available as a malware-as-a-service (MaaS) offering, is designed to harvest sensitive data such as credentials, cryptocurrency wallet information, and system details. By impersonating legitimate software and leveraging social engineering tactics, Cthulhu Stealer can compromise macOS systems and exfiltrate valuable data.

- **Type:** Information stealer designed specifically for macOS.
- **Architecture Compatibility:** Targets both x86_64 and Arm architectures.
- **Distribution:** Masquerades as legitimate software (e.g., CleanMyMac, Grand Theft Auto IV, Adobe GenP)
- **Attack Vector:** Social engineering, prompting users to enter system and MetaMask passwords
- **Data Harvesting:** Collects passwords, iCloud Keychain entries, web browser cookies, and details from Telegram accounts.
- **Exfiltration:** Stolen data is compressed into a ZIP archive and sent to a command-and-control server.
- Cthulhu Stealer uses an Apple disk image (DMG) containing two binaries for different architectures.
- It prompts users for system and MetaMask passwords using an osascript technique, similar to its predecessor, Atomic Stealer.

Impact:

- **Data Loss:** Sensitive information, including passwords, cryptocurrency wallet details, and system data, can be compromised.
- **Financial Loss:** Unauthorized access to cryptocurrency wallets and other financial accounts can lead to financial losses.
- **System Compromise:** Malware can potentially compromise the security of macOS systems, allowing for further attacks or data breaches.

INDICATORS OF COMPROMISE(IOCs):

Filename	sha256
Launch.dmg	6483094f7784c424891644a85d5535688c8969666e16a194d397dc66779b0b12
GTAIV_EarlyAccess_MACOS_Release.dmg	e3f1e91de8af95cd56ec95737669c3512f90cecbc6696579ae2be349e30327a7
AdobeGenP.dmg	f79b7cbc653696af0dbd867c0a5d47698bcfc05f63b665ad48018d2610b7e97b
Setup2024.dmg	de33b7fb6f3d77101f81822c58540c87bd7323896913130268b9ce24f8c61e24
CleanMyMac.dmg	96f80fef3323e5bc0ce067cd7a93b9739174e29f786b09357125550a033b0288

Network Indicators
89[.]208.103.185
89[.]208.103.185:4000/autocheckbytes
89[.]208.103.185:4000/notification_archive

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- **Be Cautious of Downloads:** Only download software from trusted sources. Avoid clicking on suspicious links or attachments.
- **Verify Software Authenticity:** Check for digital signatures and notarization to ensure the software is legitimate.
- **Keep Software Updated:** Install the latest security updates for macOS and all installed applications.
- **Use Strong Passwords:** Create unique and complex passwords for all accounts.
- **Enable Two-Factor Authentication:** Use two-factor authentication whenever possible to add an extra layer of security.
- **Be Wary of Phishing Attempts:** Be cautious of emails or messages asking for personal information.
- **Consider Security Software:** Use reputable security software to detect and prevent malware infections.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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