مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

macOS Malware-Cuckoo

Tracking #:432315808

Date:02-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed Cuckoo malware poses a significant threat to macOS systems, blending infostealer and spyware characteristics.

TECHNICAL DETAILS:

A newly discovered macOS malware threat named "Cuckoo." disguised as a music converter app, exhibits characteristics of both infostealing and spyware.

- **Threat Profile:** High-risk macOS malware (infostealer and spyware)
- **First Detection:** April 24, 2024
- **Delivery Method:** Disk image (DMG) downloaded from dumpmedia[.]com disguised as "DumpMediaSpotifyMusicConverter"

- **Targeted Information:**
  - Keychain data (passwords, cryptographic keys)
  - Screenshots and webcam snapshots
  - Browsing history and cookies
  - Messaging app data (WhatsApp, Telegram)
  - Cryptocurrency wallet details
  - SSH keys and other authentication credentials

- **Evasion Tactics**:
  - Encrypted network traffic
  - Conditional execution of malicious components

- **Persistence Mechanism:** Launch agent ensuring continuous operation

Indicators of Compromise:

File/IPs	Hash
Spotify-music-converter.dmg	254663d6f4968b220795e0742284f9a846f995ba66590d97562e8f19049ffd4b
DumpMediaSpotifyMusicConverter	1827db474aa94870aafdd63bdc25d61799c2f405ef94e88432e8e212dfa51ac7
TuneSoloAppleMusicConverter	d8c3c7eedd41b35a9a30a99727b9e0b47e652b8f601b58e2c20e2a7d30ce14a8
TuneFunAppleMusicConverter	39f1224d7d71100f86651012c87c181a545b0a1606edc49131730f8c5b56bdb7
FoneDogToolkitForAndroid:	a709dacc4d741926a7f04cad40a22adfc12dd7406f016dd668dd98725686a2dc
URL/IP	http://146[.]70[.]80[.]123/static[.]php
URL/IP	http://146[.]70[.]80[.]123/index[.]php
URL/IP	http://tunesolo[.]com
URL/IP	http://fonedog[.]com
URL/IP	http://tunesfun[.]com
URL/IP	http://dumpmedia[.]com
URL/IP	http://tunefab[.]com

RECOMMENDATIONS:

- Block the IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- System Updates: Ensure all macOS devices are updated to the latest version to benefit from security patches that address known vulnerabilities.
- Antivirus Software: Implement a robust antivirus solution that can detect and quarantine macOS Malware-Cuckoo or similar threats.
- Application Permissions: Scrutinize application permissions before granting access. Only authorize essential privileges to minimize malware's potential impact.
- Email Security: Be cautious of suspicious emails, especially those with attachments or URLs. Don't click on links or open attachments from untrusted sources.

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://cybersecuritynews.com/malware-cuckoo/