Malware Cuckoo – Previously Unknown Infosteler Spyware Steals Data from MacOS

Date: 03rd May 2024 | Severity: High

Summary

Security researchers have uncovered a previously undetected malware threat for macOS that exhibits characteristics of both an infostealer and spyware. Dubbed “Cuckoo” after the brood parasitic bird, this malicious code infiltrates systems and steals resources for its own gain.

Attack Vectors

The malware was first spotted on April 24th, 2024, in a Mach-O binary file disguised as “DumpMediaSpotifyMusicConverter” – an application that claims to convert music from Spotify to MP3 format. Analysis reveals Cuckoo is a universal binary capable of running on both Intel and ARM-based Macs.

The malware is delivered through a disk image (DMG) file downloaded from the dumpmedia[.]com website. Once installed, it performs a series of checks to avoid detection and determine if the infected system is a viable target.

Kandji’s researchers found that Cuckoo queries the system’s universally unique identifier (UUID) and checks the device’s locale settings. It specifically looks for systems located in Armenia, Belarus, Kazakhstan, Russia, and Ukraine – avoiding infection on machines from those regions.

Cuckoo initiates its data exfiltration and surveillance routines if deemed a viable target. The stolen data is then exfiltrated to a command-and-control server controlled by the malware operators.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• http://146[.]70[.]80[.]123/static[.]php • http://146[.]70[.]80[.]123/index[.]php • http://tunesolo[.]com • http://fonedog[.]com • http://tunesfun[.]com • http://dumpmedia[.]com • http://tunefab[.]com

File Hash	• 9254663d6f4968b220795e0742284f9a846f995ba66590d97562e8f19049ffd4b • 1827db474aa94870aafdd63bdc25d61799c2f405ef94e88432e8e212dfa51ac7 • d8c3c7eedd41b35a9a30a99727b9e0b47e652b8f601b58e2c20e2a7d30ce14a8 • 39f1224d7d71100f86651012c87c181a545b0a1606edc49131730f8c5b56bdb7 • a709dacc4d741926a7f04cad40a22adfc12dd7406f016dd668dd98725686a2dc

Recommendation

- Submit the File Hash to the Antivirus team to update their database with the file hashes.
- Submit the Domains to the Network team to update their database with the Domains.
- Keep software updated and patched.
- Use reputable anti-malware tools.
- Avoid downloading apps from untrusted sources.
- Implement endpoint detection and response (EDR) solutions.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Link

- https://cybersecuritynews.com/malware-cuckoo/