After hiatus, in-the-wild Mac backdoors are suddenly back

By Dan Goodin

Published: 2016-07-06 · Archived: 2026-04-06 15:43:51 UTC

After taking a hiatus, Mac malware is suddenly back, with three newly discovered strains that have access to Web cameras, password keychains, and pretty much every other resource on an infected machine.

The first one, dubbed Eleanor by researchers at antivirus provider Bitdefender, is hidden inside EasyDoc Converter, a malicious app that is, or at least was, available on a software download site called MacUpdate. When double clicked, EasyDoc silently installs a backdoor that provides remote access to a Mac's file system and webcam, making it possible for attackers to download files, install new apps, and watch users who are in front of an infected machine. Eleanor communicates with control servers over the Tor anonymity service to prevent them from being taken down or being used to identify the attackers.

"This type of malware is particularly dangerous as it's hard to detect and offers the attacker full control of the compromised system," Tiberius Axinte, technical leader of the Bitdefender Antimalware Lab, said in a blog post published Wednesday. "For instance, someone can lock you out of your laptop, threaten to blackmail you to restore your private files or transform your laptop into a botnet to attack other devices."

Interestingly, Eleanor won't install itself if it detects a Mac is running Little Snitch, an application firewall that can monitor and control applications' access to the Internet, researchers from fellow antivirus provider Malwarebytes reported in their own Wednesday blog post.

The second recently discovered Mac malware package is known as Keydnap. Its main function is to siphon passwords and cryptographic keys stored in a Mac's keychain feature. The developer openly lifted code from Keychaindump, a proof-of-concept app that streamlines the exfiltration of keychain contents when an attacker knows a Mac's password. Like Eleanor, Keydnap also uses Tor to contact command and control servers.

Researchers from Eset, the AV provider that disclosed the new malicious app, discovered a clever trick Keydnap developers employ to increase the chances an end user will install the malware. Once unpacked from a zip file, the installation file contains a Mach-O executable that's disguised to look like a benign text document or image file. Immediately following the .txt or .jpg extension, the developers added a space character. As a result, double-clicking on the file will launch the file in a Mac's terminal window where it can then be executed.
