Researchers at security firm Intego discover a piece of Mac malware-- OSX/Linker, an attempt at taking over a recently disclosed zero-day flaw in the macOS Gatekeeper security functionality.

The security firm also points out another potential Mac vulnerability in OSX/CrescentCore, a next-generation fake Flash Player malware redesigned to evade antivirus detection.

Publicly disclosed by Filippo Cavallarin back in May 2019, the "Mac OS X Gatekeeper Bypass" is a vulnerability affecting Gatekeeper, the technology designed to check apps downloaded from the internet for either a revoked developer signature or specific malware. According to Cavallarin, macOS treats apps loaded from a network share differently than apps downloaded from the internet. Thus, an attacker can create a symbolic link (aka "symlink") to an app hosted on a Network File System (NFS) server, before creating a .zip archive containing the symlink and getting the victim to download it. The Apple XProtect bad-download blocker fails to check such an app, Cavallarin says, making it easier for malware to infect the Mac in question.

Intego studied a total of 4 malware samples uploaded to VirusTotal on June 2019, all linked to one application on an internet-accessible NFS server.

One file was code-signed under the Apple Developer ID Matsura Fenny, a name used to sign "hundreds" of fake Flash Player files associated with the OSX/Surfbuyer adware family. As for the NFS server, the IP address point it out as hosted on a Softlayer server, although the app has been taken down since then.

Moving on to the second malware, OSX/CresentCore is a fake Flash Player updater with some extra sauce making it more difficult to detect by antivirus software (and to analyse by security specialists). For instance, if the malware detects it is running in a virtual machine (VM) or the presence of popular Mac antivirus software it simply stops working. If no antivirus software is detected, however, the malware installs either LaunchAgent, a persistent infection, the "Advanced Mac Cleaner" rogue software or a malicious Safari browser extension.

Intego says these examples of malware show how, contrary to popular belief, Macs are not invulnerable to malicious software. Attackers are constantly looking for new ways to break into Apple machines, and as such customers should always ensure their Macs are properly protected. In addition, one should warn users to never install Flash Player in 2019, not even the legitimate version, since Adobe has discontinued the software and will issue no security updates after 2020.

Go MacOS X Gatekeeper Bypass

Go OSX/Linker: New Mac Malware Attempts Zero-Day Gatekeeper Bypass

Go OSX/CrescentCore: Mac Malware Designed to Evade Antivirus