Written by Marco Attard
03 May 2017

Researchers at Check Point reveal what they believe is the first example of malware targeted at Macs-- Dok, a piece of software spreading across MacOS machines through an email phishing campaign.

The malware affects all versions of OSX and, distressingly enough, is signed with a valid developer certificate. Even worse it targets mainly European users, with phishing messages claiming supposed tax return inconsistencies found in Germany. A .zip archive dubbed Dokument.zip contains the malware, which bears the name Truesteer.AppStore.

If executed, the malware copies itself in the /Users/Shared/ folder, before executing itself from the new location by running a set of commands. It then pops up a message claiming "the package is damaged" (and cannot execute) and demands a system update. Following the "update" the malware gains full admin privileges, diverts all outgoing connections through a malicious proxy and installs more tools (Tor and Socat) to perform a man-in-the-middle attack on all traffic.

Check Point adds Mac antivirus programs are still unable to detect the DOK malware, and Apple is still to revoke the developer certificate associated with its author.

Go OSX Malware is Catching UP, and Wants to Read Your HTTPS Traffic