Featured news

OS X's Gatekeeper bypassed again

Posted on 15 January 2016.

Do you remember when, last October, Synack director of research Patrick Wardle found a simple way to evade OS X's Gatekeeper defense mechanism by bundling up a legitimate Apple-signed app with a malicious, unsigned one placed in the same directory, and wrapping it all up in an Apple disk image file?

Until they come up with a permanent fix, which will require a redesign of OS X, Apple has temporarily blocked this attack avenue by creating a (short) blacklist of files that Wardle reported could be repackaged to trip up the Gatekeeper and introduce malware on Macs.

Unfortunately, such a solution does not offer fool-proof security - Wardle has simply found a new Apple trusted file that was not on the blacklist, and which allowed him to reprise the attack.

That particular file, offered by security company Kaspersky Lab, has now been added to the blacklist, but the problem remains: Gatekeeper will let pass Apple disk images containing malicious executables if the first executable file in the bundle is not malicious. When the disk image is mounted, all the executables in the bundle will be executed, whether they are malicious or not.

Wardle is set to share more technical details about this attack in a presentation on Shmoocon this weekend, and he will also present a tool that can "generically" thwart this type of attack.

As he told Ars Technica, the tool spurs Gatekeeper to start inspecting downloaded files as soon as a new computer process is started, and the process will be stopped if the file that initiated the process is not digitally signed by an Apple-trusted developer.

Author: Zeljka Zorz, HNS Managing Editor

Apple | OS X | vulnerability

Spotlight

1 2 3 4 5

Cheap web cams can open permanent, difficult-to-spot backdoors into networks

They might seems small and relatively insignificant, but cheap wireless web cams deployed in houses and offices (and connected to home and office networks) might just be the perfect way in for attackers.

DON'T MISS

Flaw allows malicious OpenSSH servers to steal | Cheap web cams can open permanent, difficult- | 800 risk experts from 40 countries identify the top | The danger of terror attacks using drones | Have I been hacked? The indicators that

Fri, Jan 15th | users' SSH keys | to-spot backdoors | business risks | suggest you have

Back to TOP