Featured news

Compromising Macs with simple Gatekeeper bypass

Posted on 01 October 2015.

Patrick Wardle, director of research at security firm Synack, has discovered a worryingly simple way to bypass OS X's Gatekeeper defense mechanism: just bundle up a legitimate Apple-signed app with a malicious, unsigned one placed in the same directory, and wrap it all up in an Apple disk image file.

Gatekeeper, which checks apps for their provenience and disallows the running of code that's not either downloaded from the App Store or signed with an Apple developer ID, will in this case check the legitimate app and let it through, and not continue to monitor it for suspicious behavior.

Unfortunately, once that app is on the system, it executes the malicious file(s) included in the folder - and this could be any type of malware.

Wardle told Ars Technica that a variant of this attack can be executed by renaming an installer for a legitimate app and pack it with malicious plugins - Gatekeeper will only check the installer app.

He is set to present his discovery today at the Virus Bulletin conference, but has agreed to keep the identity of the legitimate app he used to perform this Trojan horse attack secret until Apple comes up with a fix for the issue.

They have known about it for the last 60 days or so, and are working on a patch. It can't be easy - as Wardle pointed out, this is not a bug, but a design flaw, and fixing it will require a redesign of the OS. But the company is ostensibly aiming for a mitigation first, and then for a complete fix.

“It’s not super complicated, but it effectively completely bypasses Gatekeeper,” Wardle told ThreatPost. “This provides hackers the ability to go back to their old tricks of infecting users via Trojans, rogue AV scams or infect applications on Pirate Bay. More worrisome to me is this would allow more sophisticated adversaries to have network access. Nation states with higher level access, they see insecure downloads, they can swap in this legitimate Apple binary and this malicious binary as well and man-in-the-middle the attack and Gatekeeper won’t protect users from it anymore.”

"Once code or content of any kind from the Web reaches the endpoint, it's game over," commented Kowsik Guruswamy, CTO for Menlo Security. "Further, the Gatekeeper bypass is significantly more severe than the recent Xcode Ghost because of this: unlike Xcode Ghost where hackers trojanized the Xcode development toolchain and placed it on a server in China for 'faster downloads,' this bypass vulnerability is an Apple-signed package downloaded from the Apple Store. And users tend to trust this blindly."

"The broader implications highlight the importance of not solely relying on static analysis, which is a moment-in-time snapshot check of good vs. bad. Even in the Web we see sites like Forbes and Huffington Post be categorized as good until one day they turn around and send malware to unsuspecting users," he noted. "As much as it's against the grain, users would be better off limiting the number of apps they are running on their devices, especially from ones that are not trusted."

Author: Zeljka Zorz, HNS Managing Editor

Follow @zeljkazorz

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.

Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.

Email @ Address Subscribe

Daily digest

Receive a daily digest of the latest security news.

Email @ Address Subscribe

DON'T MISS
Fri, Jan 15th

Flaw allows malicious OpenSSH servers to steal users' SSH keys

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

800 risk experts from 40 countries identify the top business risks

The danger of terror attacks using drones

Have I been hacked? The indicators that suggest you have

Back to TOP