Bypassing Apple's Gatekeeper

By Thomas Reed

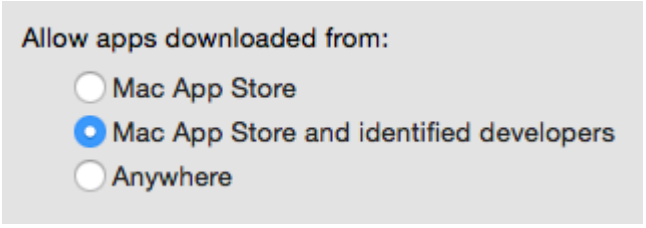
Published: 2015-10-05 · Archived: 2026-04-05 22:51:08 UTC

Ever since Apple first introduced Gatekeeper, malware creators have been trying to find a way around it.

Many different pieces of malware have done so, but at the Virus Bulletin Conference in Prague, Patrick Wardle, a security researcher at Synack, presented his findings on some new and interesting ways to skirt Apple's security.

First, let's take a look at what Gatekeeper is. OS X has a security feature called file quarantine, and when a file is downloaded by a well-behaving app, it is "quarantined." When you open a newly-downloaded application and OS X asks you if you're sure you want to open it, that's quarantine in action.

Gatekeeper is built on top of quarantine. When you try to open an app, Gatekeeper checks it out to see if it's legit. If the app isn't digitally signed, and your security settings specify that only apps signed by "identified developers" are allowed (the default setting), then Gatekeeper won't let you open it.



If you set it to the most restrictive setting, not even a digitally signed app is good enough, unless it was downloaded from the App Store. Gatekeeper will reject all others.

There have always been ways to get around the walls, though. The key to getting through the gate is understanding that the guards only check those who have already had their hands stamped, so to speak.

Specifically, in order to get stopped by Gatekeeper, an app must have been downloaded from the internet using a quarantine-savvy app, resulting in it being marked with a "quarantine flag."

An app could very easily get on your system without this flag if it were copied from a USB flash drive, optical disk, external hard drive, or even from a drive shared over the local network. This could also happen if you download an app using software that does not properly set the quarantine flag on files it downloads. (Torrent apps are frequent offenders.) In either of these cases, an app could be opened with no warnings, and without being screened by any of the built-in security in OS X.

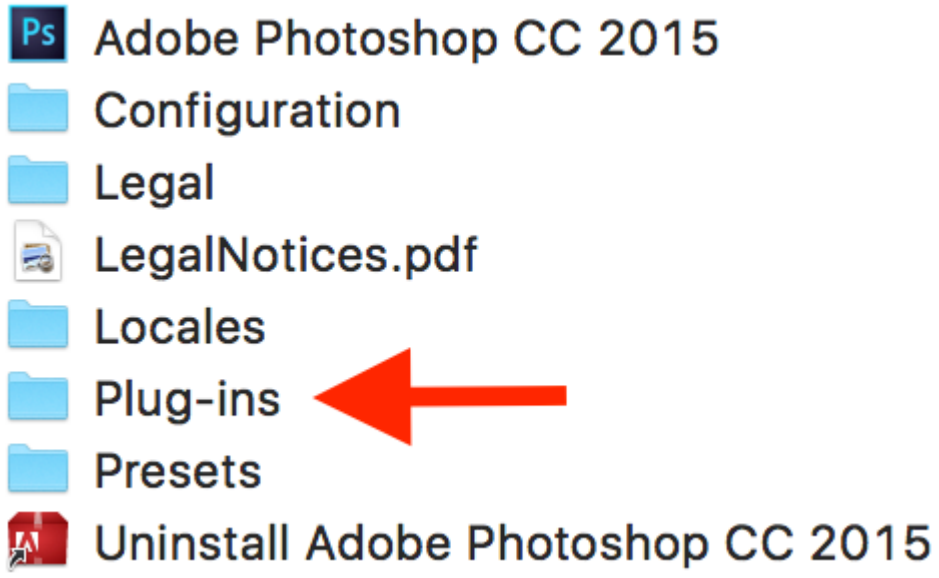
Beyond this kind of thing, vulnerabilities used to be the only other way known to bypass Gatekeeper. For example, in 2012 and 2013, there was a glut of malware that relied on Java vulnerabilities to get installed.

Because this malware was downloaded and installed behind the back of the quarantine system, it also was ably to bypass Apple's security measures.

However, Wardle has discovered a some other interesting ways to bypass Gatekeeper. In March, he wrote a paper on dylib hijacking on OS X, which allows a hacker to trick a vulnerable app into loading and executing the code in a malicious dynamic library. Packaged properly, a hacker could use a legit app as a payload to deliver malware.

A legit app would be capable passing Gatekeeper's checks, while a malicious dynamic library that it inadvertently loaded would never be examined by Gatekeeper.

At Thursday's talk in Prague, Wardle revealed yet another, similar attack vector. Some apps, including apps made by Apple, are known to load secondary "helper" apps or other executable files as needed. An example given by Wardle is Adobe Photoshop.



Photoshop will load and execute files found in its Plug-ins folder. If a hacker were to package an unmodified copy of Photoshop in a folder also containing an invisible Plug-ins folder with a malicious executable inside, that malicious code would execute without any chance of being blocked by Gatekeeper.

Worse, a hacker wouldn't necessarily need to rely on users downloading a file from a weird site. If a hacker were able to get into a privileged position between you and the server you were downloading an app from, it would be possible to substitute a modified download for the legit one.

This lowers the bar for getting malware past Gatekeeper, and unfortunately, hackers are already starting to look in this direction. The recent XcodeGhost malware, for example, involved a modified copy of Apple's Xcode software, which was made to load malicious code and, from there, was used to inadvertently create thousands of iOS apps that made it into the App Store.

As Wardle points out, it's time for Apple to make some changes to the way this system works. It's no longer good enough to only examine files with the quarantine flag before running the code inside them. There are simply too many holes in the wall, and the Gatekeeper is only watching one of them.

About the author

Had a Mac before it was cool to have Macs. Self-trained Apple security expert. Amateur photographer.

Source: https://blog.malwarebytes.com/cybercrime/2015/10/bypassing-apples-gatekeeper/