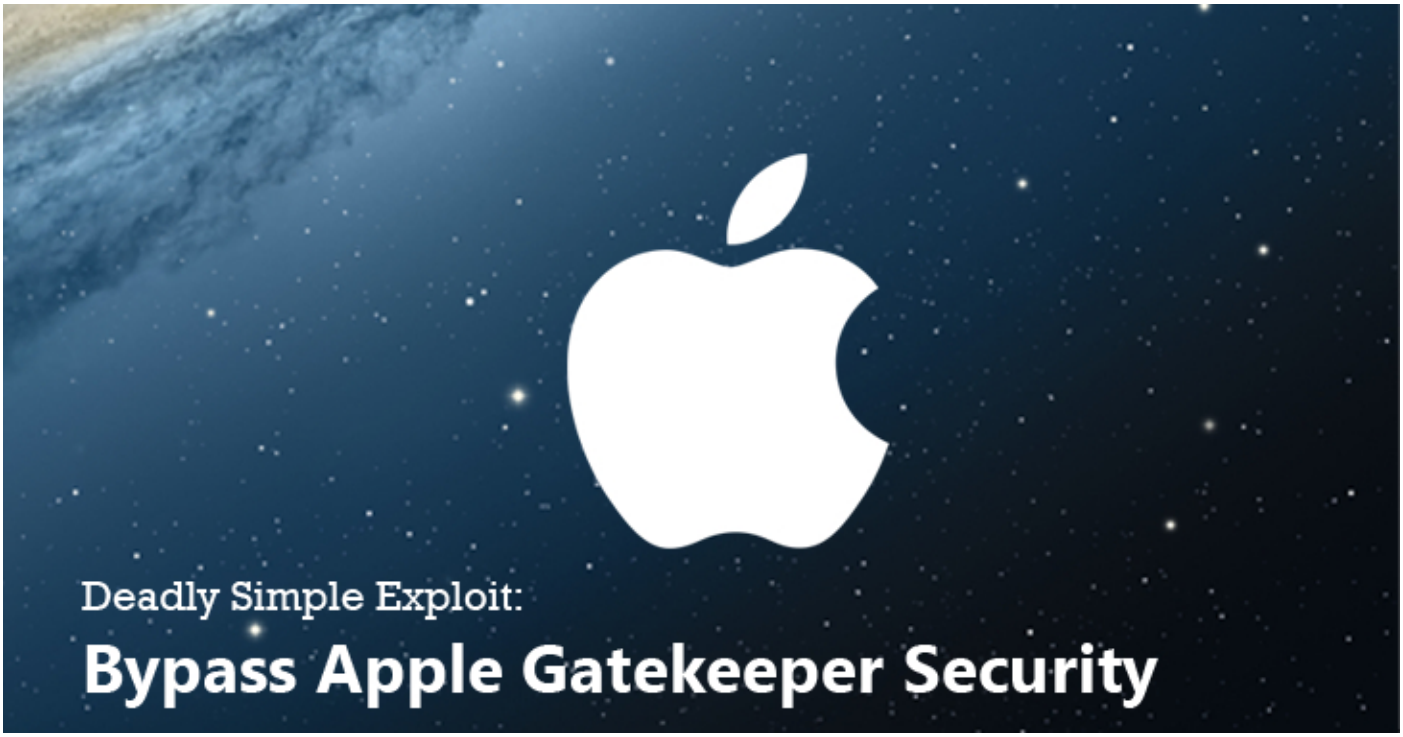
The Hacker News™
Security in a serious way

Deadly Simple Exploit Bypasses Apple Gatekeeper Security to Install Malicious Apps

Wednesday, September 30, 2015 Swati Khandelwal



Apple Mac Computers are considered to be invulnerable to malware, but the new Exploit discovered by security researchers proves it indeed quite false.

Patrick Wardle, director of research at security firm *Synack*, has found a deadly simple way that completely bypass one of the core security features in Mac OS X i.e. Gatekeeper.

Introduced in July of 2012, Gatekeeper is Apple's anti-malware feature designed to keep untrusted and malicious applications from wreaking havoc on Macs.

However, Wardle has found *a quick and simple way to trick Gatekeeper* into letting malicious apps through on Mac OS X machines, even if the protection is set to open apps downloaded only from the Mac App Store.

According to the researcher, before allowing any apps to execute on an OS X machine, Gatekeeper performs a number of checks, such as:

- Checking the initial digital certificate of a downloaded app
- Ensuring the app has been signed with an Apple-recognized developer certificate
- Ensuring the app has been originated from the official App Store

Gatekeeper's Failure

However, what Gatekeeper fails to do is – checking whether the app already trusted by OS X runs or loads other files from the same folder.

This means once Gatekeeper approved an app, it pays no more attention to what that app does. The approved app can execute one or more malicious files, which could then install a variety of malicious programs, including:

- Password loggers
- Malicious apps that capture audio and video
- Botnet software
- and many more…

The *proof-of-concept exploit* developed by Wardle does exactly the same.

How to Bypass Gatekeeper in OS X?

All Wardle has done is:

- Identified an already-signed binary file (Binary A) that runs a separate app (Binary B) located in the same folder
- Renamed Binary A
- Swapped out the legitimate Binary B with a malicious one
- Then bundled malicious file in the same folder under the same file name, Binary B

Now, Binary B needs no digital certificate or Apple developer certificate to run, so it can be used to install anything the attacker wants, completely bypassing Gatekeeper.

Same Attack Works with Plugins

Wardle said, a similar method to bypass Gatekeeper also works with plugins. All an attacker needs to do is:

- Find an application that loads plugins
- Substitute your malicious software for one of those plugins
- Again Gatekeeper will check the first installer app, and won't warn users of the malicious plugins.

Wardle's exploit works on OS X Yosemite, and all versions, including El Capitan, the upcoming release.

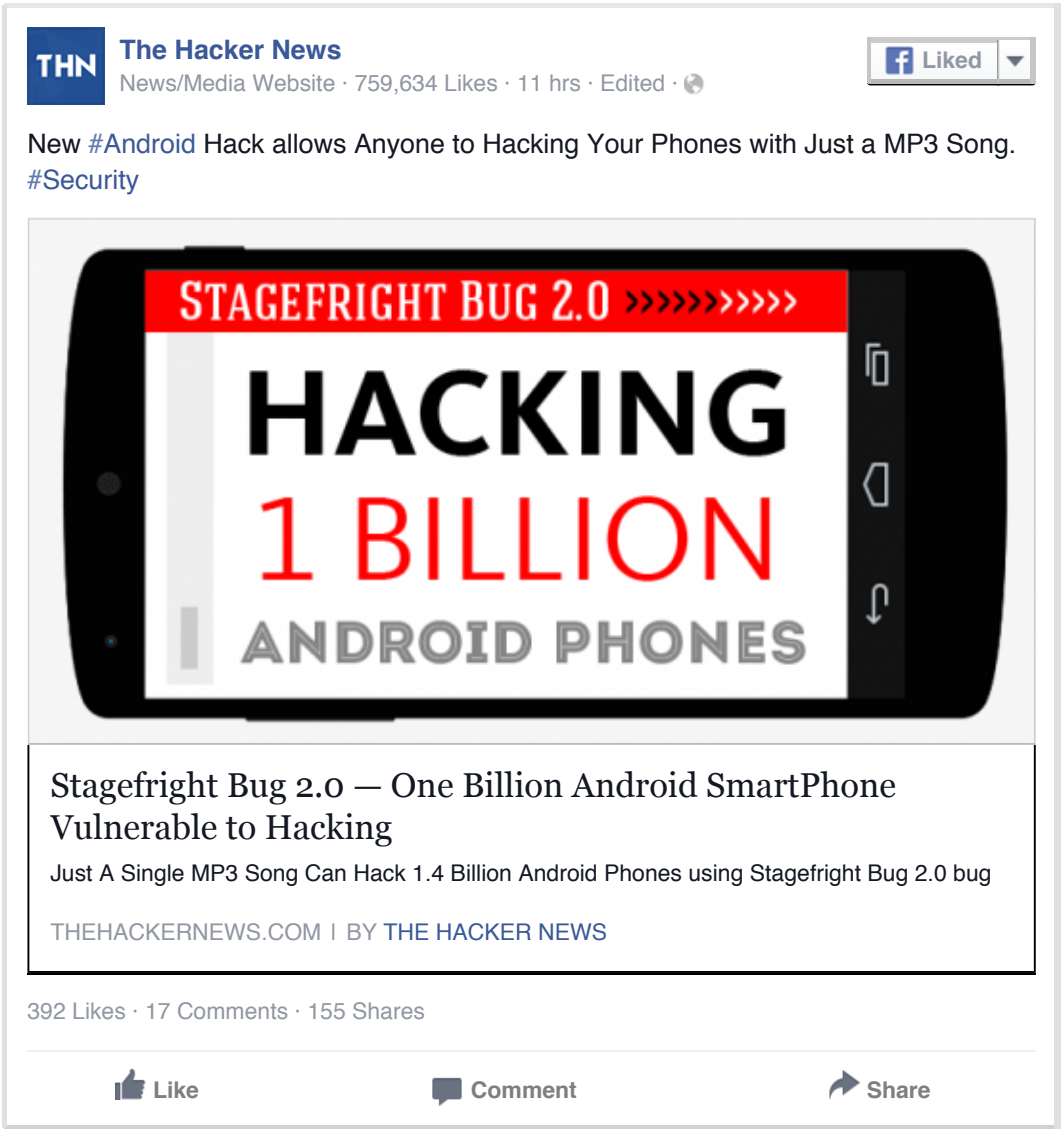
Wardle said that he tested his exploit on the most recent beta version of El Capitan – released recently to developers – and he was still able to bypass Gatekeeper.

The researcher privately alerted Apple of the Gatekeeper vulnerability more than 60 days ago,

and the company is working on a patch that will be delivered to users as soon as possible.

> *"If I can find it, you have to assume groups of hackers or more sophisticated nation states have found similar weaknesses,"* Wardle told Ars. *"I am sure there are other Apple-signed apps out there" that can also be abused to bypass Gatekeeper."*

Wardle will present his findings on Thursday at the Virus Bulletin Conference in Prague, Czech Republic.



Apple Mac Malware, Apple Mac OS, Computer Malware, Gatekeeper Mac, Gatekeeper Program, Gatekeeper Software, Gatekeeper Software Free Download, Hacking News, Vulnerability

ABOUT THE AUTHOR

Swati Khandelwal

Senior Technical Writer at Hacker News. Social Media Lover and Gadgets Girl. Speaker, Cyber Security Expert and Technical Writer.

LATEST STORIES

[How Amazon Employee bought 'Google.com' Domain for Only $12 from Google](#)

[Stagefright Bug 2.0 — One Billion Android SmartPhones Vulnerable to Hacking](#)

[Apple iOS 9.0.2 Update Patches Lock Screen Bypass Exploit](#)

[Chip-and-PIN Credit Cards and The Deadline: Here's What You need To Know](#)

[Microsoft 'Accidentally' pushed 'Test patch' Update to All Windows 7 Users](#)

[Deadly Simple Exploit Bypasses Apple Gatekeeper Security to Install Malicious Apps](#)

[TrueCrypt Encryption Software Has Two Critical Flaws: It's time to Move On](#)

[Google Play Store increases Android APK Size Limit from 50MB to 100MB](#)

COMMENTS