PHYS.ORG

Hackers have finally breached Apple's security but your iPhone's probably safe (for now)

September 25 2015, by Andrew Smith

Credit: AI-generated image (disclaimer)

Cyber security experts recently discovered that the almost impenetrable Apple App Store had been hacked. While cyber break-ins have become routine news for many companies, Apple has long prided itself on providing technology for its phones and tablets that was incredibly secure.

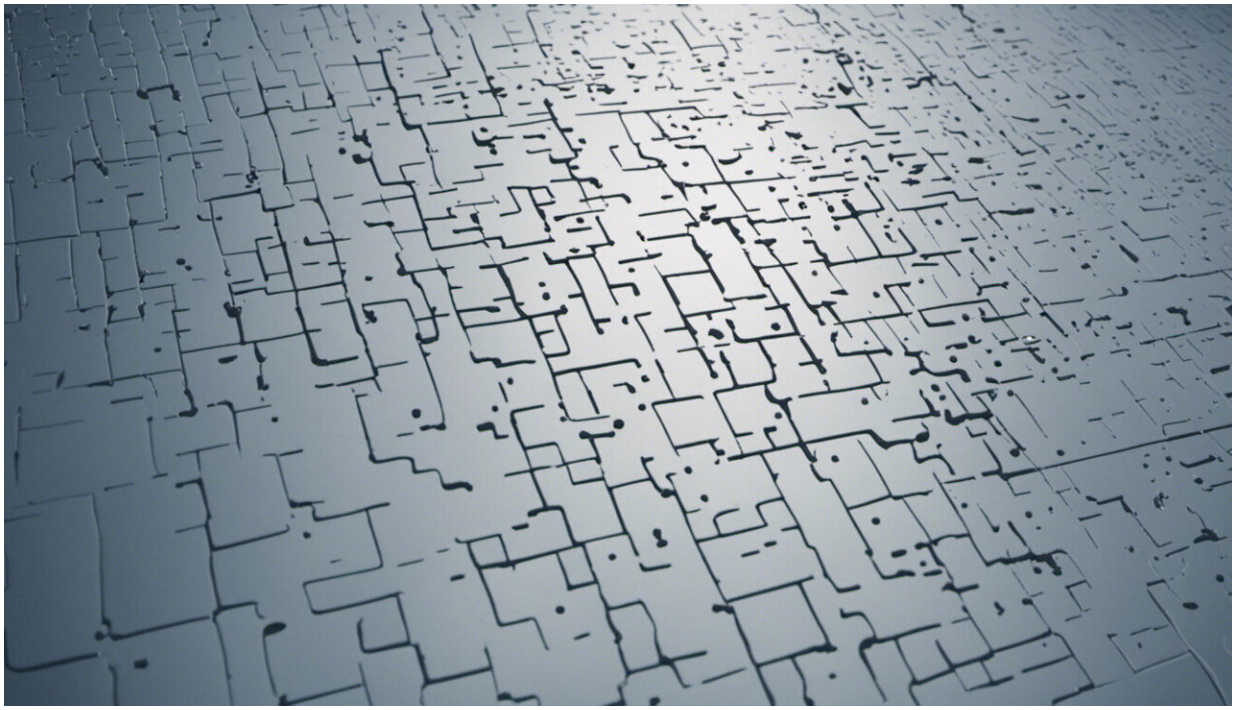
This was done by controlling how developers – the people who create your apps on your device – not only create their code but also upload it on to the app store. Steve Jobs ensured that Apple would check each app before it entered the marketplace, as well as the developers themselves, and the firm has enforced tight controls on what the devices could access.

This meant that Apple mobile products arguably were (and probably still are) the most secure you could buy. However a new attack dubbed XCodeGhost has done a great job of undermining Apple's otherwise strong security.

The attack method used was cunning and, in a technical sense, impressive. Rather than attack the devices or the App Store, the hackers compromised the Xcode framework, the underlying programming system used by developers to create the apps. This is akin to poisoning a city's water supply at its source rather than attacking the settlement's buildings or army directly.

App developers use a suite of software known as Xcode to create programs for Apple devices. Within this is a large library of functions that enable each created app to talk to the underlying phone or tablet. Each library function has different roles, from allowing you to share your location to making your phone sound like a light sabre when you wave it around.

The hackers created a malicious program (malware) that used the internet to seek out Mac computers with Xcode installed, gambling on the possibility that some of these devices were used to create apps for the Apple App store. It then dropped contaminated code library features into the Xcode system. These will appear to do what the app developers programmed them to do but also capture and send personal data from your device back to the hackers.



Credit: AI-generated image (disclaimer)

Security experts are concerned that this innovative attack leaves Apple open to future attacks. It attacks anyone who has this coding environment installed on their computer system and compromises the code before it enters the secured systems offered by Apple.

Not only is this embarrassing for the company, as their checks clearly missed this compromise. It is also embarrassing for the many developers affected as their own internal security and anti-malware processes have been compromised.

What does this mean for you?

If you are the owner of an iPhone or iPad, there is nothing you can do. Apple has never offered Apple device owners the opportunity to protect their own technology. Apple has owned this, controlled this and until recently has been very successful in protecting its products.

Android-powered devices have historically been relatively vulnerable to an excess of 40,000 types of malware. The equivalent number for Apple devices remains very low. However, this new and interesting attack means that attackers have established an alternative route into your device, through the framework used by app developers. They only need one compromised app from one compromised developer machine to be successful.

Different experts have already found multiple apps, such as Angry Birds 2, that are infected. Many of these apps are being updated in earnest by their creators to patch the security breach and new versions are automatically being installed on your iPhone or iPad. If you are ultra concerned you can delete the app and re-install in a few days time when you know it has been secured.

In order to prevent further breaches, Apple must review its security policies and how it checks all code before it enters their App Store. It also means that the onus is on all developers to improve the way they scan their own systems. Otherwise, Apple will refuse to allow them to participate in this otherwise very successful and secure system.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Hackers have finally breached Apple's security but your iPhone's probably safe (for now) (2015, September 25) retrieved 20 March 2024 from https://phys.org/news/2015-09-hackers-breached-apple-iphone-safe.html