the Availability Digest

www.availabilitydigest.com
@availabilitydig

Malware Attacks Apple Apps

October 2015

Apple fans claim that Android's open nature makes it far more susceptible to attacks by hackers. There have been many cases of the Android operating system and the smart phones within which it runs being infected with malware.

Apple's ecosystem is well known for never allowing malicious apps to reside in its iOS App Store. So long as an iPhone, iPad, MAC, or Apple Watch user purchases his apps from the Apple App Store, he is assured by Apple that his device will not be infected with some hacker's malware.

The iOS App Store Attack

This secure feeling suddenly changed in September 2015 when thousands of Apple apps were found by Internet security firms to be infected. The infections all occurred in China, which is Apple's second largest market. Chinese developers launched 130,000 new apps last year.

The infection, called XcodeGhost, hit hundreds and possibly thousands of Chinese iOS apps. They were products of some of China's most successful tech companies, and the malware affected hundreds of millions of Chinese citizens. One of the affected apps was WeChat, the popular Chinese mobile messaging utility used by 600 million people. Angry Birds 2, TenCent, and PDFReader also are on the infected list.

How Were Apple Apps Infected?

The developers of iOS apps use the Xcode utility delivered by Apple to build their apps. Xcode includes all the tools needed to develop apps for iPhones, iPads, Macs, and Apple Watches. The utility provides stringent security measures to ensure that iOS apps are secure and are not maliciously infected. This has served Apple well for decades and is a key factor in its reputation for selling only secure apps in its App Store.

However, in mid-2015, several Internet security companies detected malware of some sort lurking in iOS apps. It was Palo Alto Networks, a U.S. Internet security company, that identified the infection. Palo Alto Networks determined that Chinese developers had been using an infected version of Xcode. How had this counterfeit Xcode made it into the hands of Chinese developers?

It turns out that the root cause was the Chinese Internet infrastructure. iOS app developers are supposed to download Xcode directly from Apple's servers in the United States. However, downloading Xcode from an international source was painfully slow for Chinese tech companies. This is a result of China's censorship architecture and its weak Internet infrastructure linking it to the outside world. China controls all Internet transfers into and out of the country via its "Great Firewall," and it has made little investment in its international Internet connections.

Therefore, it became the practice of Chinese tech firms to download Xcode from local sources. Xcode was posted on several Chinese file-sharing sites for just this purpose. One such site was the file-sharing service Baidu Yunpan. As it turned out, a hacker had posted a counterfeit malicious copy of Xcode on this site. Any tech firm that downloaded Xcode from Baidu Yunpan received an infected version that would insert the malware that became known as XcodeGhost into the firm's iOS apps.

It was this lax security procedure of some of the biggest-name Chinese tech firms that allowed so many malicious apps to be made available in the Chinese iOS App Store. This is also the reason that the only compromised apps are to be found in the Chinese App Store.

What Harm Can the Malware Cause?

At first it appeared that XcodeGhost would do little damage except to steal the device ID and other information of little value to an attacker. However, upon further study, the malware was much more vicious than this.

The attacker can send commands to infected devices to steal personal information. It can conduct phishing attacks by opening up specific URLs, taking the user to infected web sites. It can read and write to the victims' clipboards, and it can post fake alerts onto the victim's screens. It can dupe customers into giving up their iCloud passwords.

Apple's Response

Apple has removed from its App Store the apps that it knows have been created with the counterfeit Xcode. It has recognized the problem that Chinese developers have downloading its tools, and it is going to make these tools available to Chinese developers from Apple servers in China. Furthermore, it will work with all developers worldwide to make sure that they are using the proper version of Xcode to build their apps.

What to Do?

The only defense against XcodeGhost is to uninstall any applications that may be infected with the malware. This affects primarily Chinese users, as it would be unusual for others to install apps from a Chinese App Store.

Some of the more popular apps that may be infected are listed in the articles entitled "XcodeGhost hack: Delete these infected iOS apps immediately" and "85 legitimate iPhone apps that were infected with malware in the big App Store hack." The articles are listed in the references below.

Summary

The Apple App Store had been almost entirely free of malware. This is the first large-scale attack on the popular software outlet. Prior to this attack, only five malicious apps have ever been found in the App Store, according to Palo Alto Networks, the U.S. Internet security firm.

It is unclear how the altered code withstood Apple's famously tough app approval process. Developers face long delays getting their apps approved and often have to wait a week or more for reviews of updates to their apps.

Acknowledgements

Material for this article was taken from the following sources:

Hack Brief: Malware Sneaks Into the Chinese iOS App Store, *Wired*; September 18, 2015.
XcodeGhost hack: Delete these infected iOS apps immediately, *Cult of Mac*; September 21, 2015.
Apple pulls infected Chinese apps from iTunes App Store, *Money.cnn*; September 21, 2015.
85 legitimate iPhone apps that were infected with malware in the big App Store hack, *BGR*; September 21, 2015.
Apple cleaning up iOS App Store after first major attack, *Yahoo Finance*; September 21, 2015.
Apple hack exposes flaws in building apps in China, *Reuters*; September 23, 2015.