Apple App Store suffers 'worst' malware attack

September 21 2015

WeChat, an instant messaging application developed by Tencent, has hundreds of millions of users in China and around the world

Hackers infiltrated the vaunted Apple ecosystem by injecting malicious software into popular Chinese mobile apps, potentially affecting hundreds of millions of users and raising security concerns as the US tech giant prepares its newest iPhone launch.

The company said Monday it had removed tainted applications from its App Store, days after security researchers revealed the breach of Apple's normally secure system which aims to weed out infected applications.

In China, more than 300 apps including the hugely popular instant messaging service WeChat and ride-hailing app Didi Kuaidi were infected with the "XcodeGhost" malware, potentially allowing access to private user data including passwords, Chinese state-run media said.

The reports were a blow to the US firm, which has Greater China as its second-largest market.

Apple told AFP that it had removed the affected apps from its online store.

"To protect our customers we've removed the apps from the App Store that we know have been created with this counterfeit software and we are working with the developers to make sure they're using the proper version of (Apple software) Xcode to rebuild their apps."

Apple's reaction came days after US-based cybersecurity firm Palo Alto Networks uncovered the flaw, saying the malware came from computer code uploaded to Baidu's cloud file-sharing service used by Chinese app developers.

Anti-censorship group Greatfire.org, which tracks Chinese Internet restrictions, called the news "the most widespread and significant spread of malware in the history of the Apple app store, anywhere in the world."

Apple, which reviews and approves each application, has generally kept its apps malware-free, analysts say.

But Alan Cockerill at the US security firm Lookout said "there are no perfect systems."

In a blog post, Cockerill said that "while Apple has traditionally done an excellent job of keeping malware out of its App Store, malicious actors are always looking for new ways to break through."

"The malicious code may have hundreds of millions of victims," Cockerill said.

Apple checks failed

Johannes Ullrich at the SANS Technology Institute said that "the real problem here is this malicious code made it past the Apple App Store check-in process."

"Apparently there is some trust between Apple and some of these developers of large applications like WeChat so these applications aren't necessarily tested as carefully if they are coming from a name-brand company," Ullrich said.

Palo Alto Networks said the malware was hidden in the Xcode software required for apps and made its way into applications without the knowledge of developers.

But once installed, the malware could allow a third party to gain access to private and personal information on an Apple device.

The malware can issue a fake dialog alert to gain access to passwords, or hijack a browser to direct users to a fake website. It can also read and write data in the user's clipboard, which could be used to get passwords, according to Palo Alto.

Only Chinese apps were known so far to have been infected—although some of those, including WeChat, are also used outside China.

Chinese apps are thought to be vulnerable because developers often bypass the official, more secure, Apple channels, which can be slowed by Chinese Internet monitoring.

Tencent, which makes the WeChat software—used by 500 million in China—said it had repaired the flaw and that there had been "no theft (or) leakage of users' information or money."

The makers of app Didi Kuaidi, which claims 200 million regular users, also reported a fix and said no user privacy was compromised.

Bad timing

Independent security consultant and researcher Graham Cluley said the incident is not all bad for Apple.

"It suggests that Apple's security is pretty good," Cluley said in a blog post.

"After all, this was quite a complicated way to get malware into the App Store."

Cluley said Apple "has a much much better track record than Google's Android one for security."

But Thomas Reed at the software firm Malwarebytes said it may hurt Apple at a delicate time.

Apple is set to release its new iPhone 6S and 6S Plus handsets on Friday in the US, China and several other key markets.

"There is little doubt that there will be some revision of the app review process at Apple as a result, but it's also certain that this incident will erode consumer confidence in the App Store as a (mostly) unassailable malware-free fortress," he wrote in a blog.