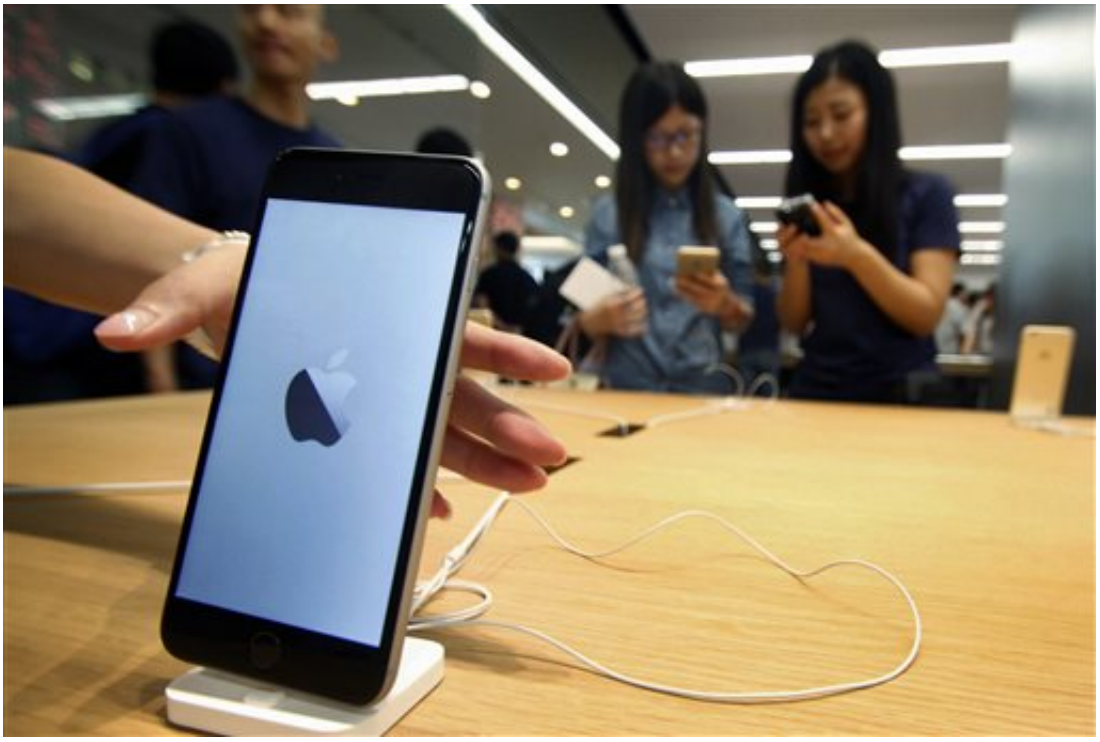
Apple withdraws some China apps after malware found

September 21 2015, byJoe Mcdonald



In this Saturday, Sept. 19, 2015 photo, Chinese women try iPhone sets at a newly-opened Apple Store in Nanjing in east China's Jiangsu province. Apple Inc. has removed some applications from its App Store after developers in China were tricked into using software tools that added malicious code in an unusual security breach. (Chinatopix via AP)

Apple Inc. has removed some applications from its App Store after developers in China were tricked into using software tools that added

malicious code in an unusual security breach.

Apple gave no details of which companies were affected. But Tencent Ltd. said its popular WeChat app was affected and the company released a new version after spotting the malicious code. Chinese news reports said others affected included banks, an airline and a popular music service.

The malicious code spread through a counterfeit version of Apple's Xcode tools used to create apps for its iPhones and iPads, according to the company. It said the counterfeit tools spread when developers obtained them from "untrusted sources" rather than directly from the company.

The malicious software collects information from infected devices and uploads it to outside servers, according to Palo Alto Networks, a U.S.-based security firm, which investigated the malware. It was first publicized last week by researchers at Alibaba Group, the e-commerce giant, who dubbed it XcodeGhost.

Cybersecurity experts say the episode shows that any device, including those running Apple's iOS software, can be vulnerable to hackers even though Apple is known for rigorously scrutinizing apps that are offered in its store.

In this Saturday, Sept. 19, 2015 photo, a man uses his iPhone to take picture as people crowd at a newly-opened Apple Store in Nanjing in east China's Jiangsu province. Apple Inc. has removed some applications from its App Store after developers in China were tricked into using software tools that added malicious code in an unusual security breach. (Chinatopix via AP)

"I wouldn't say that the floodgates for iOS malware are open now, but this vector is probably something that other attackers are going to try to replicate in the future," said Ryan Olson, director of threat intelligence for Palo Alto Networks, in an interview. He said Apple is undoubtedly working on improving its ability to block similar attempts.

Hackers are increasingly looking for new ways to target mobile apps and devices, including iPhones, because they are so widely used by many consumers, added Darren Hayes, a cyber-security expert at Pace University in New York.

The creators of this malware took advantage of public frustration with Beijing's Internet filters, which hamper access to Apple and other foreign websites. That prompts some people to use copies of foreign software or documents that are posted on websites within China to speed up access.

"Sometimes network speeds are very slow when downloading large files from Apple's servers," wrote Claud Xiao, a Palo Alto Networks researcher, on its website. Due to the large size of the Xcode file, "some Chinese developers choose to download the package from other sources or get copies from colleagues."

Companies with apps that were affected include taxi-hailing service Didi Kuaidi, Citic Industrial Bank, China Southern Airlines and the music service of NetEase, a popular Web portal, according to the newspaper Yangcheng Evening News.

The incident is the only the sixth time malicious software is known to have made it through Apple's screening process for products on its App Store, according to Xiao.