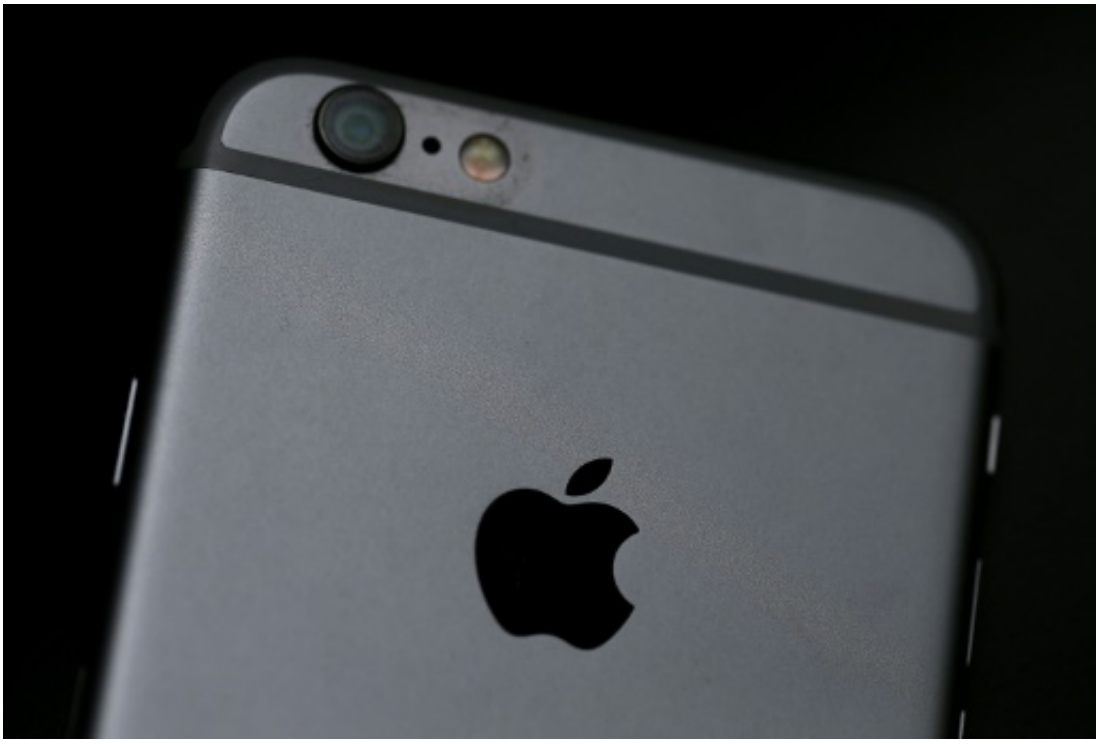
Hackers raid Apple accounts via jail-broken iPhones (Update)

September 1 2015



KeyRaider targets Apple mobile devices that have been jail-broken, or modified to be able to run applications or other software not sanctioned by the California-based maker of iPhones, iPads, and iPods

Hackers targeting jail-broken iPhones have raided more than 225,000 Apple accounts, using them for app-buying sprees or to hold phones for ransom, researchers said on Tuesday.

Jail-broken means modified to run apps not sanctioned by Apple.

"We believe this to be the largest known Apple account theft caused by malware," computer security firm Palo Alto Networks said in an blog post.

An attack using malicious code dubbed "KeyRaider" was discovered by WeipTech, an amateur technical group from Weiphone, described as one of the largest Apple fan websites in China, according to Palo Alto Networks.

In July, WeipTech members began investigating reports that some people's Apple accounts were used to make unauthorized purchases or application installations.

WeipTech worked with Palo Alto Networks to uncover KeyRaider.

KeyRaider is being distributed through Cydia repositories in China but may be affecting users in 18 countries including France, Australia, and the United States, according to Palo Alto Networks.

Cydia repositories are locations where software for jail-broken iPhones can be found and installed.

KeyRaider targets Apple mobile devices that have been jail-broken, or altered to run applications or other software not sanctioned by the California-based maker of iPhones, iPads, and iPods.

While investigating KeyRaider, WeipTech discovered an online server with passwords and other information from more than 225,000 Apple accounts, according to Palo Alto Networks.

The malicious code steals Apple account information by intercepting

iTunes traffic and App Store purchase data. It can also be used to thwart users from unlocking iPhones or iPads, according to researchers.

"In addition to stealing Apple accounts to buy apps, KeyRaider also has built-in functionality to hold iOS devices for ransom," Palo Alto Networks said.

"It's important to remember that KeyRaider only impacts jail-broken iOS devices."

In comment provided to AFP, Apple stressed that it makes a priority of security and that the App Store is curated to make sure software developers stick to guidelines set by the company.

"iOS is designed to be reliable and secure from the moment you turn on your device," an Apple official said.

"This issue only impacts those who not only have jail-broken devices, but have also downloaded malware from untrusted sources."

Apple added that it is helping those affected by KeyRaider to reset iCloud accounts with new passwords.