Malware worms its way into more apps, study finds

June 24 2014, by Rob Lever

Malicious software is increasingly making its way into mobile phones through "cloned" versions of popular apps, and software weaknesses in legitimate ones, security researchers say

Malicious software is increasingly making its way into mobile phones through "cloned" versions of popular apps, and software weaknesses in legitimate ones, security researchers said Tuesday.

McAfee Labs said in its quarterly threat assessment that weaknesses in

app security are becoming a growing problem for owners of mobile devices.

In some cases, cybercriminals can take advantage of the popularity of an app by creating a clone, which can extract personal data or even allow an attack to gain control of the device.

This was the case with "Flappy Birds," a mobile game which saw a meteoric rise but was later withdrawn by its creator.

McAfee Labs sampled 300 Flappy Bird clones and found that almost 80 percent contained malware.

"Some of the behavior we found includes making calls without the user's permission; sending, recording, and receiving SMS messages; extracting contact data; and tracking geolocation. In the worst cases, the malware gained root access, which allows uninhibited control of anything on the mobile device including confidential business information," the report said.

The McAfee report said some legitimate apps have security flaws which can be exploited by hackers.

The researchers said they discovered an Android trojan "which exploits an encryption method weakness in the popular messaging app WhatsApp" and then steals conversations and pictures stored on the device.

"Although this vulnerability has now been fixed, we can easily imagine cybercriminals continuing to look for other flaws in this well-known app," the report said.

Digital pickpockets

The researchers also said they identified malware that can steal money from a digital wallet.

One of the malware programs identified "is disguised as an update for Adobe Flash Player or another legitimate utility app," and can take over a digital wallet to send a money transfer to the attacker's server.

"Mobile malware has recently started to use legitimate apps and services, in addition to a platform's standard features, to circumvent conventional surveillance by app stores and security products," the McAfee report said.

"Consequently, protecting only the underlying platform is no longer sufficient. We believe that developers need to protect their apps and services from unauthorized and malicious use."

McAfee's Vincent Weafer said people may be lulled into a false sense of security about mobile apps.

"We tend to trust the names we know on the Internet," Weafer said.

"The year 2014 has already given us ample evidence that mobile malware developers are playing on these inclinations, to manipulate the familiar, legitimate features in the mobile apps and services we recognize and trust."

© 2014 AFP

provided for information purposes only.