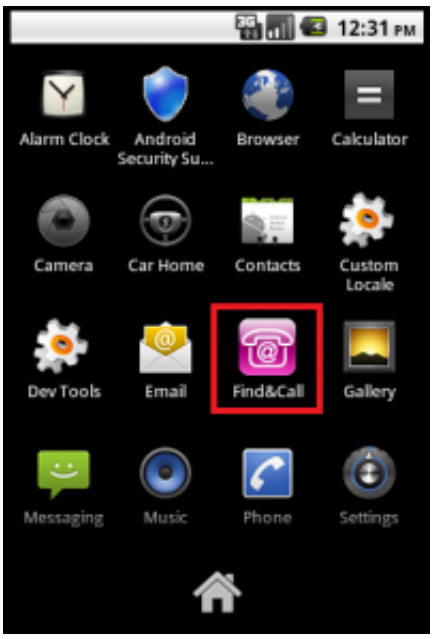
Kaspersky Lab nails 'Find and Call' trojan bearing phone-book service

July 6 2012, by Nancy Owano



(Phys.org) -- How to lose friends and de-influence people: An app called "Find and Call" has been passing itself off as a mobile phone-book helper but has been discovered to be a Trojan which, once downloaded, has all the user's address book contacts uploaded to a remote server where it proceeds to fire off SMS messages posing as the user. Find and Call was found both on the iOS App Store and Google Play store. Kaspersky Lab sounded the alarm on Thursday in a report from Kaspersky Lab expert Denis Maslennikov.

He said Kaspersky Lab had first been alerted to the malicious app by MegaFon, a mobile carrier in Russia, which said that there was a suspicious app sitting in both Apple's app store and the Google Play store.

In sending out the text messages to contacts advertising the application, the "From" field was being spoofed with the original user's mobile phone number so that the receiver of the message would assume it was from a trusted source and not spam.

Find and Call asks the user to sign in with an e-mail address and cell phone number. Kaspersky points out that neither field is checked for validity before moving forward. The user is asked if he or she wants to "find friends in a phone book." If the user proceeds, the app uploads the device's address book data without telling the user.

Trojan horses are malicious files that use social engineering, true to the word origins, presenting themselves as benign and useful gifts, so that victims will want to install them on their computers.

At first, said Maslennikov, "This seemed to be an SMS worm spread via sending short messages to all contacts stored in the phone book with the URL to itself. However, our analysis of the iOS and Android versions of the same application showed that it's not an SMS worm but a Trojan that uploads a user's phonebook to remote server."

Find and Call software was also found on the Google Play storefront for Android handsets. In the Google Play store, the app had more than 100 downloads and three 1-star ratings. In Apple's App Store, the app received 1.5 stars, according to reports.

The app may have primarily targeted Russian users as it used Russian language text in the app description, yet Find and Call was available in

app stores across the globe. Find and Call was removed from both Apple App Store and Google Play soon after the companies became aware of the problem.

One interesting point about this malware incident is that it was found both on Apple's iOS platform, which Apple tells the world has security at its core, and on Google's store. While Android is often highlighted as vulnerable to miscreants because of its open platform, the Thursday report from Kaspersky Lab indicates that all major platforms are vulnerable. Android has no monopoly on malware. As both iOS and Android grow in popularity, they will be the targets of data-stealing attempts.

Apple prides itself on its strict review process, which analyses each application that is made available for download on the App Store. Somehow this app made its way through anyway. According to reports, the app actually was there for some time. It made its first appearance in the App Store on June 13, according to MacRumors.com.

After hearing about the Trojan, however, an Apple representative issued a statement: "The Find & Call app has been removed from the App Store due to its unauthorized use of users' Address Book data, a violation of App Store guidelines." Google also removed Find and Play.

Russian blog AppleInsider.ru was able to make contact with the developer of the app. In an e-mail, he said the spontaneous sending out of SMS messages was the result of a bug discovered in beta testing and was being repaired.

https://phys.org/news/2012-07-kaspersky-lab-trojan-phone-book.html