Cybercriminals Banking on New Android Trojan

By Don Duncan, Security Engineer for NuData Security

It is estimated that there are 107.7 million Android Smartphone users in the US who have downloaded more than 65 million apps from the Google App Store, and each one of them represents a smorgasbord of opportunity for hackers to steal banking and other information.

This ample target is driving cyber criminals to continuously innovate malware and distribute it in ingenious ways. The latest malware called Android.BankBot has been cooked up using leaked banking malware source code, which was then transformed into an even more dangerous banking Trojan.

The Android.BankBot Trojan disguises itself as various Google programs with the Play Store icon fooling even savvy users into thinking that it is legitimate. Once downloaded, the app then asks for administrative permissions which most consumers click on to approve without a second thought. With permissions granted, the app covers its tracks by deleting the icon from the display screen. It also tries to connect with the command and control server to obtain account login credentials. When the door is successfully unlocked, the app automatically looks for banking credentials that might be stored in places like the Google Play Store, Uber, or Facebook etc. As added self-protection, the malware is able to divert any incoming SMS texts from the bank which would otherwise let the user know that their device has been hacked.

The result could be an empty bank account. Here are a couple of tips that Android users should employ to protect themselves:

*Never download financial applications from non-App Store sources.
*Turn off “Unknown Sources” in settings security on Android devices. Turning this feature off will disallow downloads from sources that are not known. Cybercriminals have made interfaces that are so realistic they fool even the savviest user, so while an application may look and act like it’s coming from a reputable App Store, turning off this functionality can save you from making a costly mistake.
*Conduct regular checks on your Android device to see what applications have Device Administrator rights activated.

Viruses and malware are like spices -- every day a new flavour or combination is being created by someone, somewhere, but with these ones you’ll definitely regret eating them. Maybe not right away, but someday they will catch up to you. Understanding how your device works and what resides on it will help to avoid many of the risks associated with these spicy (and dangerous) malware combinations as they evolve over time.

*https://www.statista.com/topics/876/android/
*https://www.statista.com/statistics/281106/number-of-android-app-downloads-from-google-play/

About the author:
Don Duncan is a security engineer at NuData Security. He is a veteran technologist with many years' experience working with B2C customer's technical security needs in the areas of fraud and risk management for industries such as finance, healthcare and telecom. He has previously worked at such companies as MobileIron, VMWare and HP specializing in the areas of mobility, cloud and end user computing.