WHEN *ANDROID* APPS WANT MORE THAN THEY NEED

TrendLabs
Global Technical Support & R&D Center of TREND MICRO

WHEN *ANDROID* APPS WANT MORE THAN THEY NEED

Understanding App Permissions

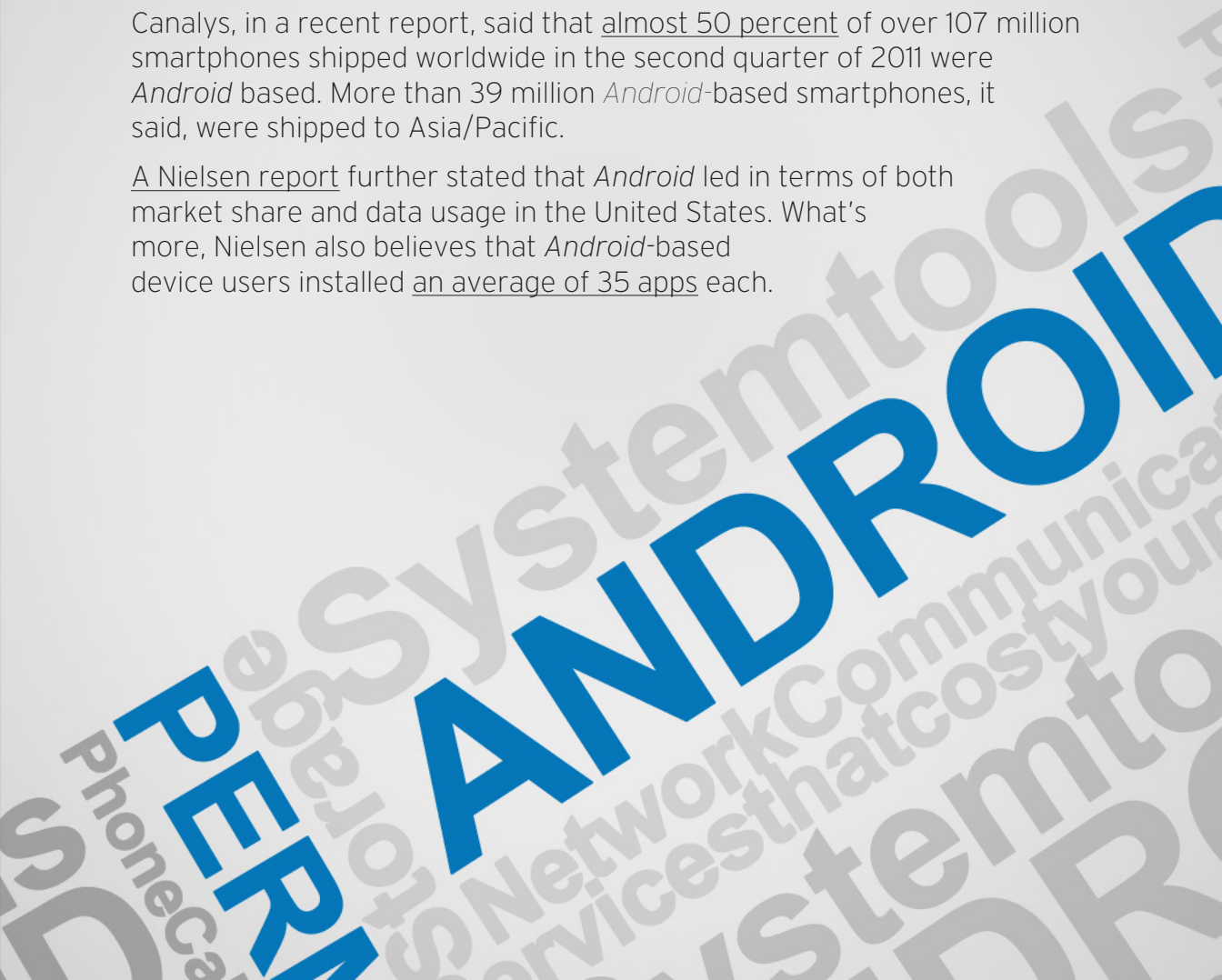
* The *Android Robot* that appears in this e-book was made available by Google under the terms of the *Creative Commons Attribution License.*

So you just bought a new Android*-based smartphone, what comes next? What else but the most exciting part—downloading the right apps to boost its functionality. You may even want to download a game or two or a movie or an MP3 player.* Android *gives you the freedom to personalize your device, which has made it attractive to those who want their smartphones to be as unique as possible.*

The freedom to personalize an *Android*-based smartphone as much as one wants and the wide variety of apps available on the *Android Market* are just two of the reasons why the OS's popularity continues to soar.

Canalys, in a recent report, said that almost 50 percent of over 107 million smartphones shipped worldwide in the second quarter of 2011 were *Android* based. More than 39 million *Android*-based smartphones, it said, were shipped to Asia/Pacific.

A Nielsen report further stated that *Android* led in terms of both market share and data usage in the United States. What's more, Nielsen also believes that *Android*-based device users installed an average of 35 apps each.



APPS SEEK PERMISSIONS IN ORDER TO WORK

Think of an Android *app as a hotel guest. Each guest gets an access card, which allows him/her to enter his/her room, the lobby, the bar, and maybe some other parts of the hotel. This card, however, does not give him/her access to the kitchen or to the hotel manager's office.*

Like a hotel guest, every *Android* app you install on your device needs certain permissions or an "access card" in order to work. The permissions you give each app tells it which of the available resources on your device it can use.

Many apps extend an *Android*-based device's functionality. As such, not all apps that seek several permissions are malicious in nature.

No single list of permissions for *Android*-based devices exists. All of the permissions that apps usually seek are, however, listed in the *Android Software Development Kit (SDK)* for app developers.

The *Android Developers* site also provides the so-called *Manifest. permission* list, which enumerates the permissions that apps basically need to work on an *Android*-based device.

Seeking users' permission to access certain features is meant to prevent the spread of malicious apps among *Android*-based devices. This is the reason why cybercriminals have resorted to Trojanizing legitimate apps in order to infect devices and to carry out malicious deeds.

At present, almost 250,000 apps are available for download in the *Android Market*. *Android's* huge user base is probably cybercriminals' main motivation for making them data theft targets.

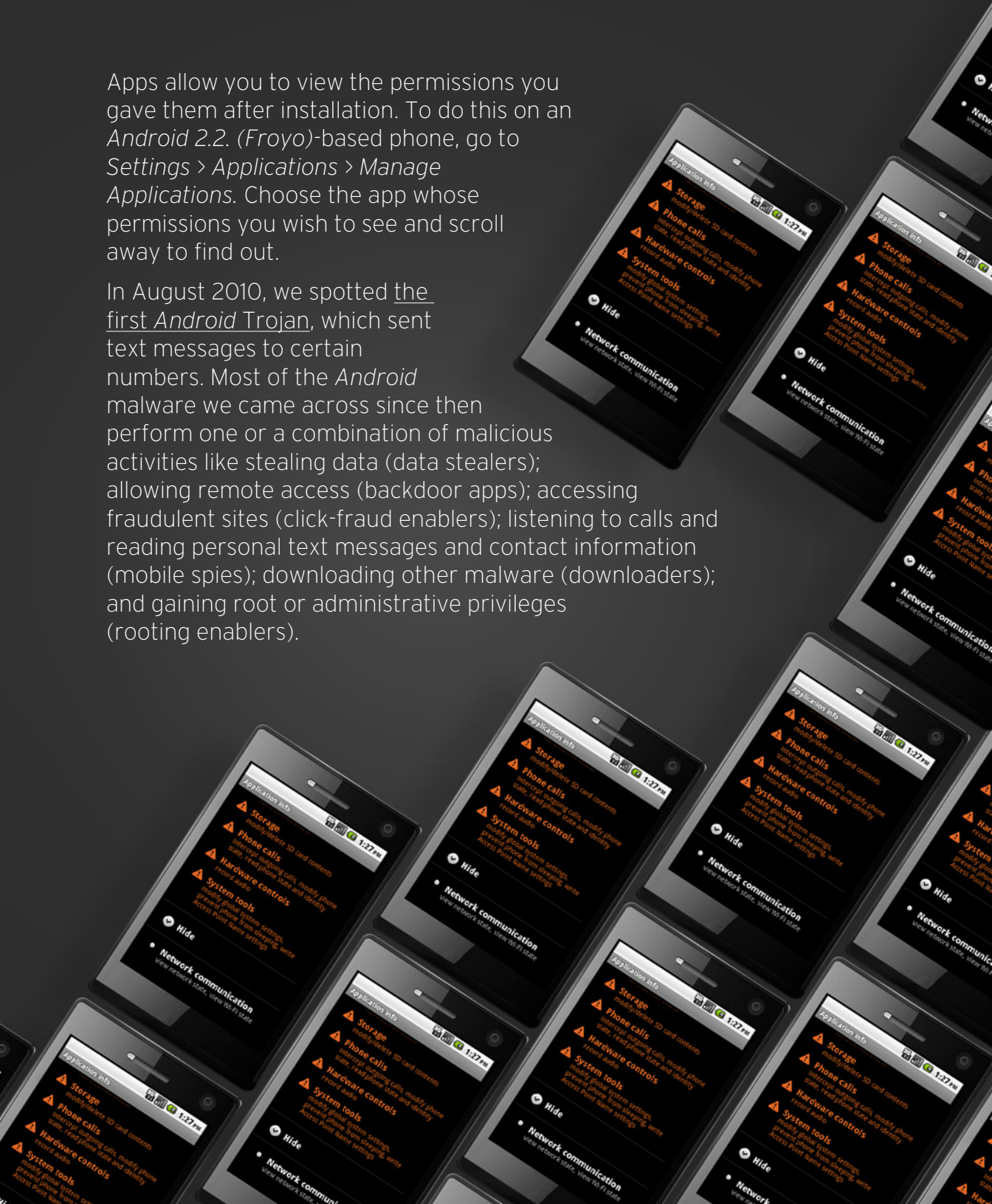
GRANTING TOO MANY PERMISSIONS CAN LEAD TO HARM

Apps ask you for certain permissions in order to work before these are even installed. Make sure you carefully read apps' end-user license agreements (EULAs), as these will give you a clear idea as to their intent. Apps rely on the permissions you grant them to do what they are supposed to.

Many apps seek your permission to grant them network access so they can download updates. Some apps seek permission to read your phone's state and identity so calls won't disrupt them from doing what they're doing. Unfortunately, these permissions can be abused by Trojanized apps to perform malicious deeds like record your conversations and send device information like International Mobile Equipment Identity (IMEI) number to a command center.

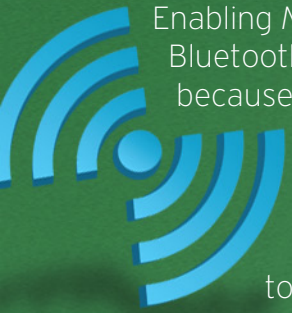
Apps allow you to view the permissions you gave them after installation. To do this on an *Android 2.2. (Froyo)*-based phone, go to *Settings* > *Applications* > *Manage Applications*. Choose the app whose permissions you wish to see and scroll away to find out.

In August 2010, we spotted the first *Android* Trojan, which sent text messages to certain numbers. Most of the *Android* malware we came across since then perform one or a combination of malicious activities like stealing data (data stealers); allowing remote access (backdoor apps); accessing fraudulent sites (click-fraud enablers); listening to calls and reading personal text messages and contact information (mobile spies); downloading other malware (downloaders); and gaining root or administrative privileges (rooting enablers).



We've listed down the permissions the Trojanized apps we've so far seen usually sought.

Network communication



Enabling *Network communication* allows apps to access the Internet or Bluetooth-enabled devices. This is the most abused *Android* permission because malicious apps need Internet access to communicate with their command centers or to download updates. Granting apps this permission allows mobile spies and data stealers to send the information they steal to remote users. Leaving your device discoverable via Bluetooth may also allow future *Android* malware to infect it like old *Symbian OS* malware.

Services that cost you money

The first *Android* Trojan abused this permission, aka *Send text messages*, along with the *Phone calls* and *Storage* permissions. Granting these allowed it to send text messages to specific premium numbers, which cost affected users a lot of money for premium services they don't even use. In this kind of ruse, the cybercriminals can pay for certain premium numbers in order to turn a profit from every text message an infected *Android*-based device sends.

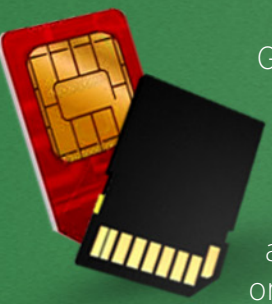
Phone calls

We've also seen malware abuse this permission to steal call logs off infected *Android*-based devices. The log file is saved as a .TXT file and sent to a command center. Call logs are favorite targets of data stealers because these provide more information on affected users. Granting malicious apps *Phone calls* permission allows them to record your conversations and steal text messages. This puts those who use their devices to conduct online banking transactions at even greater risk, as credentials given out over the phone or via SMS may land on cybercriminals' eagerly waiting hands.

System tools

Some of the malware we've seen abuse permissions like *Automatically start at boot*, *Change Wi-Fi state*, *Change network connectivity*, and *Prevent from sleeping*, which allowed them to run their own malicious services. Case in point: A game app doesn't need to automatically start every time your phone boots up so it doesn't need to seek permission to do so. In fact, this is a very strong indication that what it really wants to do is to silently run a malicious service in the background every time your phone boots up.

Storage



Granting an app permission to modify or delete your secure data (SD) card's contents allows it to read, write, and/or delete anything from it. Data stealers can abuse this permission to store a copy of the information they've stolen or to save a .TXT, an .INI, or a similar file type on your SD card before this is sent to a command center. It also gives a malicious app the capability to overwrite existing files on your SD card.

Your location

One of the more notable *Android* data stealers we found sought permission to see where the user is geographically located. Note that information like this can be used to instigate real-world crimes like stalking. Online, this may be handy when dishing out region-specific spam or malware.

Most of the Android *malware we've seen sought at least three permissions that were quite unusual for their intended use. This is a good indicator of illegitimacy when installing apps. Think very carefully about the permissions you are granting an app before actually giving your go signal. ANDROIDOS_SPYGOLD.A, which Trojanized* Fast Racing, *for instance, sought several permissions that such a game app wouldn't normally need in order to work.*

HOW TO AVOID GRANTING APPS TOO MUCH ACCESS

Remember that because Android *gives you the freedom to install any app you want, the responsibility of keeping your device malware free lies in your hands.*

For more tips and tricks on keeping your data safe from malicious apps, read our e-book, "5 Simple Steps to Secure Your Android-Based Smartphones." *Keep these three tips in mind as well to avoid granting apps too much access:*

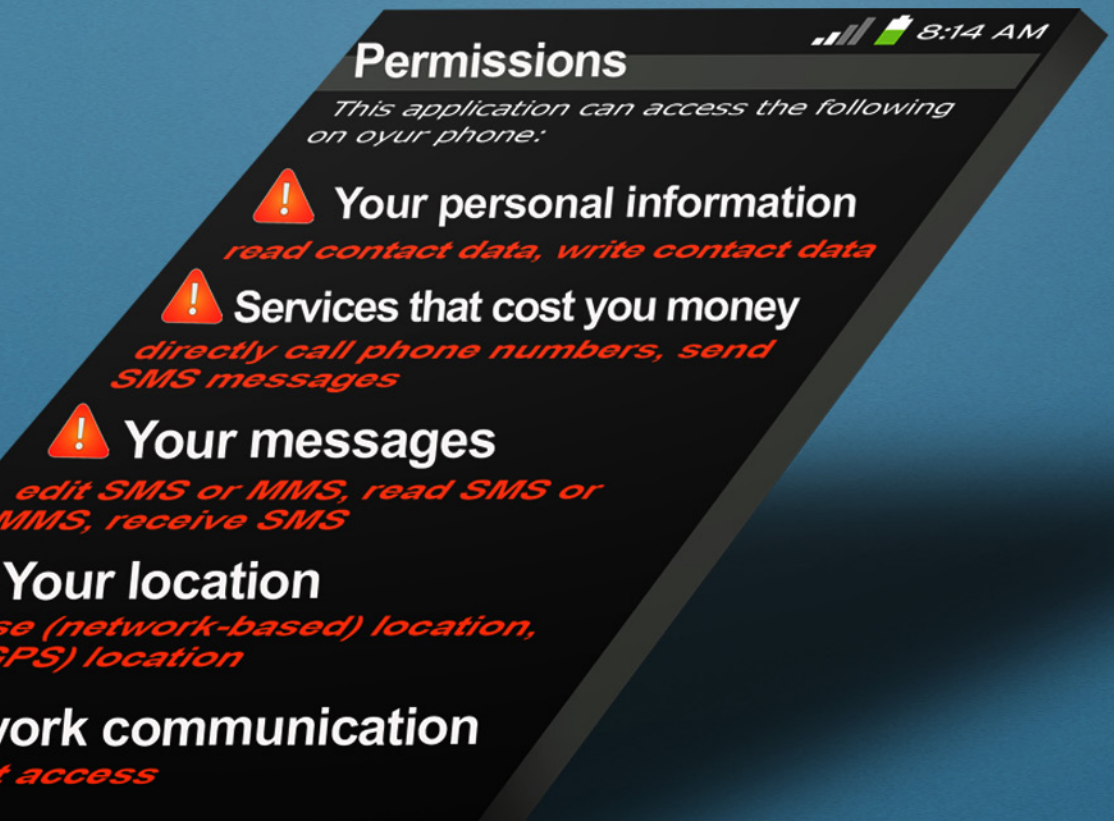
1. Read up about an app prior to downloading and installing it. Find out who created it and read what other users have to say about the app and its developer by browsing through related comments in the *Android Market* or in any third-party app store. It is also a good idea to check the app's store rating.

   Keep in mind, however, that a lot of malware Trojanize legitimate apps in order to lure users like you into downloading them.

2. Carefully read and understand the permissions an app seeks. Remember that most Trojanized apps come in the guise of legitimate ones. These just happen to seek more permissions than they actually need in order to work.

   If you downloaded and installed a media player, for instance, that seeks permission to send text messages, think again before accepting its terms of agreement. Even though some legitimate apps seek several permissions, there is such a thing as asking for too many permissions that can put your device and your data in grave danger.

3. Investing in a mobile security software that protects not just your phone but also the data stored in it is also a great idea. Solutions like *Trend Micro™ Mobile Security Personal Edition* can identify and stop malware before these even reach your phone. Backed by the same technologies behind the Trend Micro™ Smart Protection Network™, it effectively protects your *Android*-based devices against the latest malware.



TREND MICRO™

Trend Micro, Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our website at **www.trendmicro.com.**

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com

Securing Your Journey to the Cloud