Chapter 10

Malware and Spyware

Like the personal computer, the mobile smartphone is susceptible to various types of malware. Throughout this chapter, I will refer to malware and spyware collectively as malware. Even though I do this, it is essential to know the difference between each of these types of hostile applications.

**Malware** is defined as any piece of malicious software that lives on a user’s computer or smartphone whose sole task is to cause destruction of data, steal personal information, or gain access to system resources in order to gain full control of the device it is on. Malware is written with the sole intent of causing harm; and usually, malware authors will write the malware to target a specific weakness in an operating system or platform. Often, the malware author will want to maximize the spread of her malware and will look to implement a mechanism where his software can copy itself to other, similar devices.

**Spyware** is a term used to refer to malware that accesses and exfiltrates personal or private information from a device. For instance, in the case of mobile phone malware, the application may be after an end user’s e-mail messages, contact list, SMS messages, or even photos. Spyware generally needs to be stealthy and stay on the device for long periods. Thus, spyware authors will aim to perform little or no disruptive activity on the device, so that the end user is not aware of her data being stolen. Just about anyone can use malware; it is no longer a requirement that you know how to code the malware yourself.

Many companies sell malware to individuals, large corporations, or even governments (see the case study later on in this chapter). I have seen two types of companies selling malware: the ones that sell to large organizations or governments and the ones that sell to individual retail consumers. As we will review later in this chapter, one large Middle Eastern telecommunications provider was caught spying on its entire BlackBerry subscriber base. The software that helped do this was sold by a well known US company that specializes in legal interception. It turns out that the source code was completely developed from scratch, and its sole purpose was to capture and exfiltrate e-mail messages from an infected device.

On the other end of the spectrum, you will find the malware or spyware packaged and sold to any individual who is willing to spy on someone that she knows. In most cases, the companies that sell this type of software will proclaim “Catch cheating spouses!” Apparently, this is quite appealing to some folks! I will also look at one of these versions of *retail malware* in some detail.
Four Stages of Malware

We can classify malware operations into four different, but distinct, stages. While not formal, these stages have been visible in most instances where malware has been discovered on devices.

**Infection**

This is the stage where the malware is introduced to the device. The holy grail of infection is one where no end-user interaction is involved. This occurs when malware can be copied to a device by something as harmless as sending a user an SMS message or compromising the device when it is on a wireless network.

The second method of infection is through a partially assisted action. The user is asked to click a link in a malicious website. Once he does this, the malware will copy itself to the device. An attacker sends this link to a user in an SMS or e-mail message. While effective, this requires user intervention; in most cases, diligent users will always be suspicious about clicking random links sent to them.

The last form of infection occurs when an attacker will physically copy the malware to the device, either through a USB port or via browsing to a website. This takes place in instances where the attacker and end user know each other, or the attacker has physical access to the end user’s device. This technique is not effective if a user has password protected his device and requires a password to use it or install applications on it.

**Compromise**

Most often, infection and compromise go hand in hand. In this context, I am using the word compromise to describe how the malware is able to gain super-user access to the device. As a result, the malware can make changes to the device configuration in any manner it chooses to do so—and without requiring device-owner interaction.

As we saw in previous chapters, programs running on Android will require a user to grant it explicit permissions to access facilities like the Internet or read e-mail messages. During the compromise stage, the malware will use a weakness in the operating system to circumvent the permission granting process, thereby allowing it to execute any function without the user being aware.

**Spread**

Unless specifically targeted at an individual, a malware author will typically want to infect a large number of users. He may want to control an army of devices or just access private information from many different people. The Zeus Trojan (found on the personal computer platforms) will spread using weaknesses found in the operating system. Its sole purpose is to collect a user’s keystrokes and collect credentials to banking and social networking websites.