A new botnet agent has surfaced in the past couple of months that takes control of your Android smart phone and starts sending out SMS messages, and if you pay by the text, then get ready for a pretty tall bill. The botnet, called SpamSoldier, is relatively simple at this time, but researchers are warning that future versions could become quite the issue to take down and remove from the device. But the researchers did note that “This sort of attack changes the economics of SMS spam.” Using this botnet, a spammer can lay the cost of spam SMS messaging onto the owner of the infected device.

How It’s Getting Around

Most often the botnet is spread through supposedly free versions of gaming apps that are advertised via an SMS sent to the victim. People downloading the free versions of “Need For Speed” and “Angry Birds Space” have been hit the most often, but there have been other apps reported to contain SpamSoldier. Once downloaded the application will get the user to grant permissions of all types, including access to the SMS functions, and phone books, and will in turn convert the phone into a SMS spamming monster.

How SpamSoldier Works

Once in place the botnet sets itself up as a service on the phone, so rebooting will only refresh the bot, not stop it. When SpanSoldier gets started, it will contact a Command and Control server, (C&C,) and acquires the SMS message to be sent out along with a list of 50 or so numbers. The bot will then start sending text messages, waiting exactly 1.3 seconds in between texts. Additionally, the bot is scheduled to check back to the C&C server every 65 seconds to get new messages, and more phone numbers. And, as I said at the beginning of this hub, if you pay for the individual text message then expect to see this reflected on your bill.

Evolution Of The Botnet

Cloudmark reports that the bot came out of the closet in the end of October masked as a mobile anti-malware solution. The sites that made it available were hosted in Hong Kong on a server that also offered free games. But in early November the botnet was hidden in the free games. In the last couple of weeks the spammer has increased activities so far peaking out at a half a million texts per day. So far though, the distribution has been limited, but all carriers have been affected. Lookout’s security alert said, “The potential impact to mobile networks may be significant.” Not to mention what it could “potentially” do to your cell phone bill.

As with computers, the operating systems of Android cell phones and tablets can be hacked under your nose when you import and install programs. Your personal information can also be compromised. The Android operating system is certainly not immune to these types of intrusions. There are over a dozen different ways that rogue android applications can cause problems.

In this article, I go over things you should notice and steps that you can take to prevent yourself from having problems. I also discuss the usefulness of antivirus and malware prevention programs for andoid operating systems. Lastly, there is a video and discussion of anti-theft applications like Cerberus. All of these measures will show you how to protect your valuable Android cell phone or tablet.

Avoiding Malware Tips

These are some basic principles of going about using your phone, downloading apps and observing application behavior that will decrease the likelihood of infections or having your personal information compromised:

1. Avoid downloading any application that has less than a thousand downloads. Also check the ratings of users to verify the usefulness and validity of the program. Correspondingly, it is important for you to participate in application ratings for the better good of the android community.

2. Everyone probably knows by now that there are two reliable vendors of android applications, the Google Play Store and Amazon Appstore for Android. Use these sources for downloads of programs as they regularly check for malware. This doesn't mean that there is a possibility of bad apps still being on their site, as recent history attests. But it does mean that the probability of loading apps containing malware is less. Note that Android phones can also be set to prevent downloading from unknown, or unmoderated, web sites.

3. Don't just download apps randomly because they are cheap or free. Check out the reviews of the apps online to see if they have features and functionality that you want. Reviewed programs are a safer bet for your device.

4. Sometimes you can come across apps that may have a little different spelling than the

specific app you are looking for. Avoid these apps, as it has been observed that a high percentage of them are malware.

5. When installing an application, observe whether the program requests for permissions that it normally would not need, like sending SMS messages or having access to your system, wifi or your network. Don't install programs that request for services that you deem as not essential to the application on your device.

telefon dinleme