

Recent Malware Threats



mobilesecurity.com [[San Francisco, CA](#)] During the Super Bowl this year, all eyes were on the grand finale of one America's favorite sports: football. Capitalizing on the hype and attention, malware was recently released and detected that was disguised as the mobile version of Madden NFL 12, one of the most popular and successful gaming franchises in the US.

The malware was actually a premium rate SMS Trojan, which did a few nasty things:

- First, it does not load the football game, but it does infect your device with a trojan that includes code allowing the sending and receiving of SMS or text messages.
- The trojan, known as Android.FoncySMS, detects the country you're in from the SIM card and then sends a text to the premium rate number corresponding to the device's country.
- Lastly, the trojan will install code that acts as a bot and will try to contact an external IRC server.

If you want to know more about this, read the blog entry on [Connect](#).

Pretty nasty, right?

The developers of these trojans and malware are sneaky and take advantage of what's popular out there. Late last year, the trojan named Android.Fakenetflix was released that looked very similar to the real Netflix app for Android. What made it potentially dangerous is that Netflix is a very popular service, and up to that point only a select few devices were able to get the Netflix

app. Naturally, word gets out that there's a Netflix app that allows you to stream your Netflix queue through your device, people will flock to get it.

In reality, the app was fake. Once a user submitted their email and password, nothing happened. Analysis revealed that the trojan only collected this information and sent it to a remote server. Anyone who entered in their Netflix credentials was now at risk of their Netflix account being hacked. In terms of Netflix, this is nothing more than a nuisance and has no direct financial repercussions. However, there are probably many people who use the same email/password combination on many sites. The combinations entered here could be attempted on thousands of websites – chances are there would be a few successful hits.

It's pretty scary to think what these apps can do if you're not careful. Most apps are completely harmless. Fortunately, there are some basic things you can do to protect yourself from most of these malicious apps.

10 Tips to protect consumers against cell phone cybercrime:

1. Password protect your phone
2. Enable encryption on the phone if it is available to further protect your data
3. Be diligent about app permissions on all new installed apps and upgrades (you can compare permissions here)
4. Don't click on unsolicited links – they may take you to phishing sites
5. Check your phone bill regularly for unusual premium call or SMS charges
6. Use anti-theft software to remotely lock & wipe your phone when lost or stolen
7. You can use security software (e.g. Norton Mobile Security) to safeguard your phone against malware and spam
8. You should exercise the same level of caution you do on a PC or laptop when you encounter a strange SMS/MMS message or an unsolicited Bluetooth connection request
9. Backup your phone's data at least once a month
10. Record your phone's specific ID ahead of time (phone #, carrier, make, model, SIM card #, IMEI, etc.)

Mobilesecurity