Amateur Season for Bad App Developers

mobilesecurity.com [San Francisco, CA] Once upon a time we might have assumed that every Android smartphone owner would be a pretty tech-savvy guy. Rather like with Linux 15 years ago – when everyone used Windows, right? Except graphic designers, photographers and anyone working at Pixar – they were the Mac guys. Well things have changed pretty dramatically in the PC world – Linux remains mostly confined to sysadmins, geeks and vegans (including one individual on the FBI's Most Wanted list) – the same could

also be said about the mobile market.

10 years ago, no one had even heard of iPhone (Apple wouldn't begin its development until 2005, the same year Android Inc. was acquired by Google). It's no surprise that cybercriminals are still playing catch-up when it comes to finding ways to exploit mobile technologies to gather information, disrupt services and make money.

Symantec's latest Internet Security Threat Report recently reported that 315 mobile vulnerabilities were discovered in 2011 – an increase of 93% on the previous year's total. This is significant year-on-year growth, but the total number of vulnerabilities doesn't sound particularly terrifying. A sign of what may be around the corner comes from a recent concern affecting Japanese Android users.

A malware author using a single common piece of code has persuaded at least 70,000 users to install a malicious app that harvests various details including their name, phone number and email addresses from the phone's contacts.

So how did this individual or organization trick so many users with these dodgy-looking apps? Well, they're employing the same tactics that are increasingly being used on desktop and laptop PCs across the globe – by mimicking popular, genuine applications to confuse users to provide access to their private information.

According to Joji Hamada in Symantec's Security Response blog, 29 separate apps have been discovered from 7 app developers that mimic popular games in Japan (or play a video that relates to the game). Once installed and opened, these apps connect to an external server and dump private information that might subsequently be sold to criminal groups. They get access to this private information by requesting a few more permissions than should reasonably be required by the app, so the user has basically opened the front door and allowed the criminal to walk right in and take what he likes.

One thing users can be aware of in order to protect themselves from this particular threat is to pay attention to permissions when installing or updating their apps. Another red flag that something is not quite as it should be is that the name of the app is different when displayed on the phone to the name under which it's offered on Google Play.

This is just sloppy development, and provides yet another example of how important it is for android users to be vigilant. Look for signs that the app didn't go through the full QA process prior to release on the market, actually stop for ten seconds to check the permissions you're allowing when you install an app, and check the name of the app developer – if you're downloading a popular app, then there's a high chance a quick online search will reveal some details about the source – and these simple steps can hold the key to not becoming a victim of mobile cybercrime.