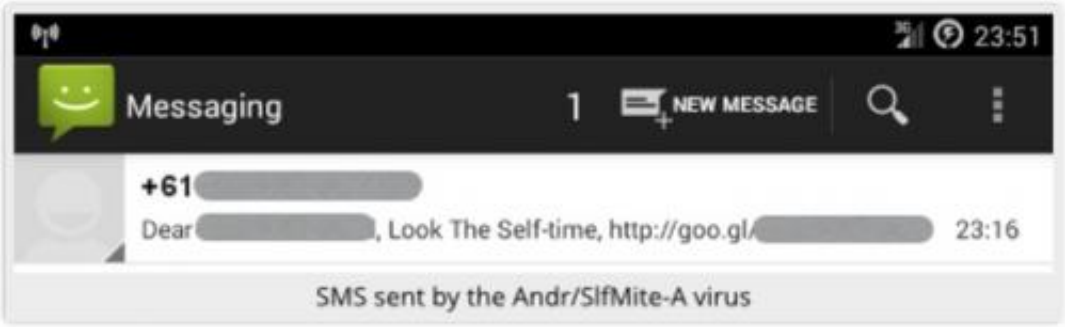
Time to watch out for SMS worms on Android devices

July 1 2014, by Andrew Smith



Google's Android now dominates 80% of the smart phone market. Of the major phone operating systems, Android is the most vulnerable to security breaches and yet perceptions haven't caught up with reality. People simply aren't as worried, or as careful, as they ought to be.

If you're using an Android and aren't too concerned, maybe a recent announcement by a leading anti-malware company will make you stop and think. When were you last suspicious of a text from a friend?

Well, now is the time to start checking your messages with more scepticism as a virus known as "Andr/SlfMite-A" has been spreading throughout the Android world, transmitted by text messages, also known as SMS.

If you are fooled into clicking on a link embedded within the SMS, and if your phone is unprotected, the virus will in turn be installed on your own phone. The virus will then attempt to send text messages to your first 20 contacts. The message may look something like this:

By making your contacts think this message is from you and is therefore a genuine (and seemingly honest) text message which they must act upon. It tricks them into clicking the link, unleashing malware onto their phone. And so on.

If this all sounds familiar, it is because self-replicating "worms" like these were a feature of early mass-market online viruses. A decade ago, famed worms such as ILOVEYOU or Mydoom spread through email, shutting down computer systems throughout the world and causing millions of pounds in damage.

Today's SMS spam is spread in the same way, but things move even faster now. As soon as anyone clicks on the link, they become part of the worm's progress. You may only be one victim with 20 contacts, but these things soon add up. If all 20 contacts fell for the link once every hour, the worm could have swamped the entire planet and all its Android devices within a day.

Fortunately not everyone falls for this, nor do all the text messages get through. In the end, Andr/SlfMite-A is likely to fizzle out. However, whether it is successful in infecting your friends, the virus also downloads a small malware application which appears to direct users towards Mobogenie, an independent Android app store.

It is important to note that Mobogenie has been hit in the past by other malware issues. There's a reason the anti-malware community don't consider it an effective resource for protecting your smart phone.

Should I panic?

If you already have an anti-malware application installed on your android smart phone, just check to see that its malware definitions are up to date. Then rest easy and make yourself a nice refreshing drink.

But if you do not have any protection I would be very concerned and strongly advise that you consider installing an antivirus app.

If you do get a mysterious text message from one of your contacts my best advice is to phone them and ask if they intended to send a message. If it looks as if they may be infected, point them to this article and advise them to ensure that their phone is protected.

Android is a victim of its success

Any computer and any operating system is potentially vulnerable to malicious code. So long as unsuspecting souls can be persuaded to download applications for their own personal benefit, cybercriminals will be able to exploit systems and create all kinds of mayhem.

Sadly, research has shown that over half of us could be persuaded to download malware for the right price. In some cases, manufacturers have managed to stem the supply: Apple and Microsoft, for instance, retain tight control over their smart phone app stores, ensuring a high degree of safety.

But the reality is that cybercriminals tend to target popular systems, and Android is increasingly dominant. There are many naive people out there, and more than one way to install dodgy apps.

It is important that everyone using any technology becomes more aware

of the different types of attacks out there as you cannot entirely rely on experts to protect your smart phone from every attack.

We don't all use our phones in the same way so nor are we all exposed to the same degree of risk. The way you respond to texts, emails or browser messages, the sites you visit and the applications you may download all have an effect on the security of your smart phone.

Becoming cautious should be a way of life. There is nothing wrong with checking to see if an unusual text message from a friend is suspicious; who knows, maybe they'll even appreciate hearing your voice.

Source: The Conversation