Freebie tricksters unleash spam botnet using Android phones

December 20 2012, by Nancy Owano

(Phys.org)—Cloudmark, a San Francisco based messaging security company, posted a notice on Sunday that an Android trojan is being used to create simple havoc, aka an SMS spam botnet. Cyber-thieves dangling the lure of free access to popular games such as Angry Birds Space and Need for Speed Most Wanted are staging attacks for the purpose of turning victims' Android phones into spam-sending monsters. Smartphone security company, Lookout, also based in San Francisco, is referring to the spammer botnet as SpamSoldier. The company also warned that it is spread through SMS messages that advertise free versions of paid games.

Once the user clicks on a link from one of these SMS messages, an application is downloaded that claims to install the game. The user unwittingly activates the SpamSoldier trojan.

This is a mobile botnet created to infect phones so as to spread spam. In this instance, the spam-forwarding trigger is lurking behind the lure of free versions of popular Android games. The app contacts a web server for a list of phone numbers and can then start sending a flood of text messages. In addition to the game lure, security watchers say infected-phone messages also try to rope in victims by telling them they won a gift card.

Users falling for the scam download apps from a server. They are told to grant the app permission to install and give it the ability to browse the web and send texts. While this should raise suspicions as trouble-bound directives, some users are not phased, said Andrew Conway of Cloudmark: "Not many people read the fine print when installing Android applications."

Once installed, that trojan will begin connections to the command and control server. The "zombie" waits 1.3 seconds after sending each message, and checks with the C&C server every 65 seconds for more numbers. Lookout, meanwhile, has noticed instances of the SpamSoldier on all the major carrier networks in the U.S., and warns that affected users may experience lower speeds along with higher bills. The single infection vector appears to be spam SMS messages. According to Lookout, it has not yet detected SpamSoldier on any major app stores.

Given the large amounts of SMS messages sent, this may not only add up to user costs but also slowdowns, according to Lookout's Derek Halliday. Similarly, Cloudmark's Conway said, "You better have an unlimited message plan or your phone bill may come as a bit of a shock."

The obvious admonishment would be not to download anything from unfamiliar sites. In a Tuesday update, Conway had this additional advice to offer: "So, if you do get SMS spam, don't bother replying STOP to the sender, just forward that message to 7726." The 7726 is SPAM on the keypad and hitting 7726 is designed to stop text-message spam by reporting it to the phone user's carrier. Cloudmark is continuing to monitor this attack, according to Conway.

More information: blog.cloudmark.com/2012/12/18/ … -sms-spambot-update/