

Subex Telecom Fraud Alerts

March 2011

Hackers run up huge texting bills by adding malicious 'features' to legitimate smartphone apps

A malicious Android app has been doing the rounds, which is capable of hijacking a smartphone and running huge texting bills without the owner even knowing it.

This particular compromised Android app is known as Steamy Window. The Steamy Window is a free program that Chinese hackers have modified and re-released into the wild. The cyber criminals grab a copy of Steamy Windows, and then add a backdoor Trojan horse - "Android.Pjapps" by Symantec's label -- to the app's code. This reworked app is then placed on unsanctioned third-party "app stores" where unsuspecting or careless Android smartphone users find it, download it and install it.

The Trojan planted by the infected Steamy Windows, send messages to premium rate numbers for which hackers are paid a commission. It also has a built-in filter that blocks incoming texts from the user's carrier, a trick it uses to keep victims in the dark about the invisible texting. The trojan monitors inbound SMS texts, and blocks alerts telling the users that they have already exceeded their quota. This way, the smartphone owners remain unaware of the charges they've racked up texting premium services until they receive their next statement.

The Trojan can install other applications, monkey with the phone's browser bookmarks, and surreptitiously navigate to Web sites apart from silently sending text messages.

Android smartphones are an attractive target for hackers, because of their increasing popularity and ability to install apps downloaded from third-party distribution sites. Operators should warn smartphone owners of downloading from unauthorized app stores and also carefully look at the permissions the app requests when it is getting installed.

**Source: COMPUTERWORLD, Feb 2011*

Fraudster makes \$8 million through international computer hacking

A man in New Hampshire was arrested and will be sentenced for his role in an international computer hacking conspiracy through which he made \$8 million.

According to the government's evidence, the fraudster and his co-conspirators infected German citizens' computers with a program that would force the computers' telephone modems to surreptitiously dial premium telephone numbers rented from German telephone companies by the fraudster's co-conspirators. The premium telephone numbers were like 1-900 numbers which are used for directory assistance or astrological predictions. The telephone companies charged victims for added expenses on top of standard connection fees and sent a portion of the added expenses to those who rented the premium lines (fraudster's co-conspirators). The victims were unaware that they were being charged extra as a result of their computers' telephone modems calling these numbers. The victims generally paid these additional charges if they did not notice them on their telephone bills.

The telephone companies would then send the added charges to the premium telephone line renters, who divided the proceeds amongst themselves and the main conspirator. The man from New Hampshire (conspirator) participated in this fraud by employing computer programmers to write and edit the computer hacking software and by sending the hacking software to co-conspirators.

Although the conspirator participated in the scheme while based in Massachusetts and elsewhere in New England, computers or computer users from United States were not targeted. Instead, they focused solely on computers in Germany and possibly other European countries. In the process, from 2003 through 2007, the fraudsters made approximately \$8 Million from the computer hacking conspiracy.

Operators are advised to warn their customers regarding such potential threats, and track high volumes of calls into specific premium rate service numbers

**Source: United States Attorney's Office, District of Massachusetts, Feb 2011*

Telecom operator in Ghana busts SIM Box fraud operation

A well known telecom operator in Ghana and the Criminal Investigations Division (CID) of the Ghana Police Service busted yet another SIM box fraud operation. This bust led to the seizure of SIM-box equipment worth \$200,000, but the number of fraudulent SIM cards involved is still unclear; however all those SIM cards have been blocked.

SIM box fraud is a set-up in which some fraudsters connive with cohorts abroad to route international calls through a VOIP system and terminate those calls through local phone numbers in Ghana to make it appear as if the call is a local call. Telecom operators and the state consequently lose a lot of revenue through such calls.

According to the Telco, this particular SIM box operation was causing financial losses in excess of GHS2.5 million per month since December 2010. So far, the telecom operator had blocked over 90 per cent of the fraudulent SIM cards on its network and continues to do so.

**Source: Modern Ghana, March 2011*

For all previous fraud alerts click on the following link: <http://www.subexworld.com/fraud-alerts.html>