Subex Telecom Fraud Alerts

July -September 2011

$ 750,000 per month Telecom Piracy Ring busted

Haitian police executed the largest bust in the history of Haitian National Police (PNH), which led to a series of arrests including the vice president of a local telecom operator. The PNH was able to bust a $750,000 per month telecom fraud with the help of the Carribean Telecommunications giant. The telecom operator provided information pertaining to fraudulent numbers suspected of circumventing normal telephonic exchange carriers and avoiding communications charges. This is a common form of bypass fraud.

The PNH's Anti -Telecommunication Fraud (ATF) unit along with National Council of Communications (CONATEL) initiated a raid on two suspicious properties .The properties were found to have equipment typical of a bypass operation and the equipment was seized. Five arrests were made and several warrants for arrest were issued. In total, 9 simulation boxes, 11 outdoor antennas and a host of routers, power cells and regulators were seized. According to CONATEL, the loss to the carriers and the state is estimated at $750,000 per month.

Operators should note that bypass fraud does not appear to be slowing, so proper monitoring and controls must continue to be rigorously implemented.

**Source: defend.ht, Aug 2011*

Overseas fraudsters dupe a telecom operator's call center staff

A local telecom operator's call center was duped by overseas scammers posing as legitimate customers. The operator said it knew of nine customers who had fraudsters' mobile phones connected to their accounts without their knowledge. The operator suspected that the numbers were set up to then run up large bills on unsuspecting customers' accounts.

The fraudsters posed as employees of the telecom operator and contacted people on their mobile phones to find out if they were on a pre-paid or post-paid plan. Those who identified themselves as post-paid plan users were told they had won a $50 credit and were asked for personal details such as their full name, address and date of birth. These details were then used to dupe the operator's call centre staff. Staff unwittingly transferred new numbers to a handset held by the fraudster.

The telecom operator is now working with the Communications Fraud Control Association (CFCA)—an organization based in the United States—to determine the origins of the fraud and reasons as to why New Zealand numbers were targeted. The operator has also warned customers not to divulge personal details and be wary of any incoming calls from unexpected international numbers.

Modus Operandi

- Fraudsters call mobiles and pretend to be employees of the telecom operator.
- They promise $50 credit and take personal details.
- The details are used to dupe call center staff into setting up additional numbers.
- These new numbers are transferred to handsets held by fraudsters.
- These phones are then used to charge large bills to victims' accounts.

Operators should be alert to such threats and proactively educate their customers so that they don't fall prey to such scams.

**Source: nzherald.co.nz, July 2011*

HippoSMS, the latest SMS Trojan to hit Androids

As communicated in our previous fraud alerts, the Android applications' market seems to become more vulnerable to Trojans every day. The latest to hit Android smartphones is HippoSMS. This Trojan is sophisticated enough to automatically send SMS communications to expensive Premium Rate Numbers and to prevent the service provider from notifying users of the charges incurred. The HippoSMS gets embedded inside an application that looks legitimate and activates as soon as the application is installed on the Android device. The Trojan then monitors incoming SMS communications and deletes all messages that come from the mobile service provider. Service providers typically send users notification messages about the user's account, such as the current balance. By deleting the messages, the Trojan ensures that users don't find out about the costly text messages until the final bill arrives.

So far the threat of HippoSMS is limited only to users in China where the malware is hard-coded to send messages to a specific number. However, this type of mobile malware (that sends stealthy text messages to expensive prime-rate numbers) is becoming a serious problem in Russia, China and the Ukraine, where it's easy to rent out these numbers.

Operators are advised to keep a vigilant eye on such Trojans and also inform customers to be careful while downloading mobile applications.

**Source: eWEEK.com, July 2011*

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