Subex Telecom Fraud Alerts

October-December 2011

Major African operator loses $9 million to SIM box fraud

A major African operator lost over $9million to SIM box fraud from March to October in 2011. The amount represented revenue for 70.48 million minutes of overseas calls. These were fraudulently routed through SIM Boxes and made to appear on the operator's network as local calls. This also resulted in the government losing $ 4million in taxes.

According to a source belonging to the operator, the direct international calls dropped by a whopping 15.7million from 49.18 million in March, 2011 to 33.48 million in October, 2011. Most of these international calls were terminated on the operator's network as local calls using SIM boxes containing the SIM cards of 'less vigilant' telecom operators. According to the National Communication Authority (NCA) in September, 2011, it detected around 5,454 SIMs being used for SIM boxing.

Apart from the loss of money, the SIM Box problem has also made it difficult for customers to call back on the missed calls received from relatives, friends and business partners abroad as the number that appeared on their phone was usually a local number.

SIM box problem is growing at a rampant rate and operators must be vigilant and must use effective controls to prevent SIM box fraud.

**Source: business.myjoyonline.com, Nov 2011*

Terrorists fund PBX hacking in the US

The FBI revealed last week, that four hackers – 3 men and 1 woman, were arrested in the Philippines in connection with organizing PBX attacks on the business clients of a major telecom operator in the US. Reports also suggested that the hacking was funded by terrorists linked to an Al Qaeda group that carried out the Bali bombings in 2002 killing 202 people.

The hackers carried out PBX attacks on the operator's clients by gaining access into the operator's network and then used the PBX's to generate calls to premium rate numbers. The revenue generated from the hacking was diverted to the accounts of terrorists who paid the hackers a commission for their activities. Due the PBX hacking, the operator is said to have suffered a loss of $ 2million.

It is a matter of great concern, that this the first time terrorists have funded a PBX attack.

Operators are advised to educate their customers and be wary of such attacks being funded by terrorists.

**Source: infosecurity-magazine.com, Nov'11*

PRS Trojan targets Android users in Europe and Canada

A new Android Trojan masked as an SMS monitoring application is targeting users in Europe and Canada. The Trojan found by Kaspersky , dubbed as Trojan-SMS.AndroidOS.Foncy appeared sometime in September. This malware is advertised as an application for monitoring SMS messages and is distributed via a file hosting website. Once installed on the device, the fake app sends four text messages to predefined premium-rate numbers in France, Belgium, Switzerland, Luxembourg, Germany, Spain, the U.K. and Canada, depending on the country corresponding to the SIM card.

Earlier such Trojans were rampant in China and Russia as installing apps from unofficial sources was very common but now these have spread to European countries and Canada.

In another similar incident, 22 applications were removed from the Android Market after they were found to contain fraudulent software. This RuFraud Scam as it is called, would make the users believe they are downloading a legitimate game or program but instead it was giving their phones permission to send text messages to premium rate numbers which cost about Euro3 per message.

According to reports, this fraud is said to have originated in Russia.

Operators should advise their customers regarding downloading of apps from legitimate sites and educate them about such Trojans.

**Source: CSOOnline.com, Nov'11 and BBC news, Dec'11*

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