Subex Telecom Fraud Alerts

July-September 2012

Telecom fraud ring busted in Taiwan and Philippines

Taiwan and Philippines authorities busted the largest telecom fraud ring which led to the arrest of 357 fraudsters. During the bust, the authorities found telecom equipment and a list of the victims who were targeted for fraud.

The fraudsters impersonated as law enforcement officers and tricked the victims into believing that their bank accounts were being used for money laundering. They then convinced the victims to transfer money into the fraud ring. The fraudsters would be indicted for illegal use of telecommunication equipment and fraud.

Operators are advised to keep their customers informed of such instances so that they would be wary of fraudsters who pose as actual authorities.

**Source: Focus Taiwan, August 2012*

Toll fraud -the most menacing of mobile malware attacks

A toll fraud program called "FakeInst" has been doing the rounds among users of smartphones and duping them of a lot of money. This toll fraud program prompts smartphones to send bogus premium text messages. The charges for these messages are then added to telecom service bills. The money from this malware goes to the fraudsters.

The Toll fraud malware is designed to hide what it is doing, and charges go unnoticed in complex mobile service billing tstatements. The victims find out only upon receiving their bill statement. Also this malware is targeted at victims who use premium SMS services.

The malware FakeInst poses as an installer for legit apps like Opera and WhatsApp Messenger. It is steadily on the rise and according to Lookout it represented 82% of malware detections.

Operators should educate their customers to be aware of such malwares and not download apps from untrusted sources.

**Source: dark Reading, France 24, September 2012*

Third SIM BOX fraud syndicate busted in Ghana

A major telecommunication provider in Ghana was successful in busting a SIM box fraud syndicate for the third time. The operator worked closely with the Criminal Investigation Department of the Ghana police.

The team uncovered two hyper media SIM gateway equipment, each with the capacity to accommodate 160 SIM cards and a large quantity of SIM cards. They also confiscated two industrial batteries, several antennae, two modem hubs and other gadgets.

In the SIM box fraud set up, fraudsters connive with partners abroad to route international calls through the internet using voice over internet protocol (VOIP) and terminate those calls through a local phone number in Ghana to make it appear like a local call.

The caller is often unaware of the activities of these fraudsters. These SIM boxes result in a lot of revenue loss to both the operator and the state.

Operators should note that SIM box fraud is still growing rampantly and efforts should be made to shut them down.

**Source: Ghana Broadcasting Corporation, August 2012*

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

To follow active discussions on various topics log on to or subscribe to: Telecom Fraud Professional Group LinkedIn, @SubexTweets and Subex Blog