Subex Telecom Fraud Alerts

January - March 2013

Police nab members of syndicate involved in Bypass fraud racket in Manilla, Philipines

The National Capital Region Police Office reported the arrest of two members of a syndicate that uses computers and other devices to convert inbound international calls to local calls, shortchanging telecommunications companies, and the Philippine government, of millions of pesos in revenue.

With networked devices, the syndicate allows calls to bypass the telecom operator's gateway facility. The syndicate converts the international caller's number into a local cell phone number, so the call will be charged local instead of international rates.

The syndicate's "hotline" would be printed on call cards abroad sold by "foreign brokers." The hotline instructs callers on how to call the syndicate's Philippine operations. When the Philippine-based operations receive the call, it uses the operator's SIMs to forward the calls to the Philippines-based recipients. The syndicate earns through "profit-sharing" especially with the call cards' sales, he said.

Operators should note that bypass fraud is on the rise and measures should be taken to counter them effectively.

**Source: Inquirer Global Nation, February 8th 2013*

International Revenue Share Scheme (IRSS) hits Uganda

Telecoms in Uganda have busted a huge fraud scheme perpetuated by an international gang of criminals.

Fraudsters travelled from abroad and buy local SIM cards of the different telecoms. In Uganda, the fraudsters bought SIM cards of all the top operators. They then travelled out of the country to Sierra Leone where they negotiated an international roaming deal with one of the telecom companies. They also travelled to Latvia. After negotiating with small telecom operators in Latvia, they used a computer application to generate fraudulent calls to Latvia.

The fraudsters set up a fake system which generated multiple overlapping roaming long duration calls to Latvia. They generated long duration calls and made them to be multiple so as to maximize their revenue.

The telecom operator in Latvia would issue a bill to the local operators in Uganda for terminating their long distance international calls. This scheme operated as if a Ugandan subscriber is roaming in Sierra Leone but calling Latvia subscribers. The Sierra Leon operator would also bill the Uganda local provider for enabling their customers to roam on their network. The fraudsters had negotiated with the operators in Latvia and Sierra Leon to share the spoils once the Ugandan operators sent the payments.

Telecom operators should understand the need for appropriate technology to monitor telecom network to enable them to detect unusual customer behavior.

**Source: Summit Consulting 10th February 2013*

PBX hacking of 3 corporate clients results in bills running up to $100,000 in India

An international call scam, that appears to have breached the security of a major operator's networks installed in three companies, has left the operator clueless about recovering bill amounts running into hundreds of thousands of dollars from its affected clients.

International calls of varying durations (from a couple of minutes to about half an hour), to destinations such as Somalia, Ethiopia, Poland, Guinea and Seychelles, were made from these firms during February, leading to generation of bills with a total value of over $100,000.

Officials said that such a huge volume of international calls is highly unlikely to be an inside job and are certain that it is a case of ISDN facilities being compromised.

Operators should ensure implementation of fraud management systems to keep a tab on the sudden surges in international call traffic.

**Source: The Hindu, March 24th 2013*

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