Subex Telecom Fraud Alerts

September 2010

Mainland China, Taiwan police bust major telecom scam

Chinese Mainland and Taiwan police jointly busted a major telecom fraud group and arrested 451 suspects. Amongst those arrested, 186 were from Taiwan, one was a Hong Kong native and the remainder were from the Chinese mainland.

In May, police found out that the fraudsters had rented an overseas server and set up a telecommunications fraud network in southeast China's Fujian Province. This fraudulent network provided number changes, batch calls and other technical services to cheat consumers. According to the police, the group consisted of three parts: a technical support team to power the online fraud network and rent it to other fraudulent groups; a so-called "information consulting company" responsible for making fraudulent calls; and an underground bank that transferred illicit money in the name of fund management services. The group bosses of this fraud network were said to be based in Taiwan.

Source: Hindustan times, Aug'10

UK police dismantles £1.2m international telecom fraud ring

Police arrested nine people suspected of being involved in a criminal ring that stole £1.2m (over $1.8m) from telecommunication companies. The fraud involved buying hundreds of iPhones worth up to £599 each and using the SIM cards to call premium rate numbers around the clock.

Police claim that a group of West African fraudsters used cloned credit cards and stolen identities to buy iPhones and associated service subscriptions over the Internet. However, instead of shipping the devices to the addresses specified during purchase, they were delivered by corrupt drivers to an individual, who received almost 1,000 iPhones in this manner.

The fraudster removed the SIM cards from the devices and sold them to a gang, made up primarily of Pakistani nationals. This gang then shipped the cards to countries in the Middle East, Europe and Asia, where they were being placed inside special auto-dialler devices configured to call local premium rate lines continuously.

Through this method, the fraudsters managed to steal £1.2 million in July from a UK telecom provider. In this case, the operator instantly settled charged with the premium rate numbers operators, but when they tried to recover call charges from customers, they discovered that those customers did not exist.

Source: London Evening Standard, SOFTPEDIA, Aug'10

Two senior telecom officials caught for $1.5m telecom fraud

In what could turn out to be a big scam for the Indian telecom industry, the police recently unearthed a well-laid conspiracy to dupe a major Indian telecom operator in Mumbai, of crores of rupees. The police arrested two senior officials and nine distributors in connection with the scam, which is estimated to be Rs7 crore ($1.5m).

According to the police, deputy general manager-GSM service, assistant general manager-sales and the distributors issued three hundred thousand mobile phone connections between June 2008 and February 2009, most of which were based on fake or forged documents.

According to the police, the motive for this fraud was to reap the benefits of a scheme which was recently launched by the telecom behemoth. The telecom operator had floated a scheme named SIM-75 in which SIM cards of Rs75 were provided to the operator's distributors on an upfront commission of Rs50 per card. Under this scheme, the distributors were entitled to a commission of Rs150 for each activated connection up to 600 connections, Rs200 for 600-2,000 connections and Rs250 for 2,000-and-above connections. The only clause in the scheme was that this would be applicable to a minimum 100 activations per distributor and recharge of Rs100 on the activated connections.

The fraudsters misused this scheme and issued fake connections. Proper verification of documents, which is a prerequisite while issuing the connection, was also flouted. According to police the operator's senior officials did not ensure that the distributors adhered to the prescribed conditions to avail the incentives. Based on their knowledge, the distributors activated thousands of fake connections based on forged and fictitious customer application forms and claimed huge amounts of commission against the connections.

Source: Daily News & Analysis, Aug'10

Feds crack $15m phone clone scam

Federal prosecutors uncovered a scam that used tens of thousands of cloned cell phones to defraud a large American telecom operator out of $15m in lost long distance revenue.

The operation started in the latter half of 2009, when cellular customers began complaining that they were billed for international calls they didn't make. When the operator looked into the matter, they discovered that many of the calls were made from locations hundreds of miles away from where the customers lived. Also the duration was within minutes of other calls made from the customers' homes.

Eventually, the operator discovered that electronic credentials belonging to "tens of thousands of its customers" were used to make international calls that would have cost $15m had they been billed at the going rate. Also, many of the defrauded customers' online accounts were breached so that changes could be made to passwords, international calling features and other settings.

The fraud surfaced when nine employees belonging to the operator were accused of illegally accessing customer accounts more than 16,000 times between January and June of this year. Among the information they took were the mobile station ID and the electronic serial number that are used to uniquely identify each handset on the network. By plugging the credentials into new cell phones, the fraudsters were able to make phone calls that were charged to the accounts of the defrauded customers

Source: The Register, Sep'10

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