Telecom Fraud Alerts

April - June 2015

Spanish police bust 'Premium Rate Text Messaging' racket worth €5 million

Spanish police have busted a gang that they say made at least €5 million over the last decade from a premium-rate text-messaging scam.

The gang is suspected of sending out hundreds of thousands of SMS and WhatsApp messages each month, aimed at luring recepients into replying using a premium rate number. Each sent message would cost the user around €1.50, with the revenue being shared with the mobile network operator.

The gang's network consisted of two SMS Premium companies, which acted as a front-end for around 20 bogus companies used to launder money. Currently there are 213 premium rate operators in Spain with around 1,500 numbers and the percentage of these companies that are using the numbers for fraudulent purposes is increasing.

**Source: http://elpais.com/*

East African operator loses USD 33 million to telecom fraud

A large East African telecom operator is reported to have lost around USD33 million to telecom fraud. A national security agency announced that at least USD 33.6. Million had been swindled by about 55 individuals over the past year.

The agency that reported the national security report, referenced it to "sophisticated technological devices" that could imply the use of GSM Boxes to bypass heavy international call charges.

**Source: http://www.cellular-news.com/*

VoIP systems owned by UK businesses attacked by hackers

UK businesses are getting disproportionately targeted by a surge of attacks against Voice over IP (VoIP) systems. The growing use of VoIP technology in business and a greater availability of tools that make hacking easier has led to an increase in attacks worldwide.

UK-based systems are being hit particularly hard, according to a new study by a renowned security consultancy. During the first quarter of 2015, researchers observed a large amount of VoIP attacks worldwide; however, the majority were against UK servers.

VoIP attacks often started just a few minutes after a new server went live and it is found that 88 per cent of VoIP attacks took place outside of regular working hours, when there would typically be no staff present to monitor the situation. Service abuse and toll fraud have long been the most common objective of VoIP hackers. Premium Rate Service (PRS) fraud is becoming more and more prevalent as well.

A large number of calls to premium numbers and foreign numbers were recorded and such actions can have serious financial impacts on the organization being attacked. Also, the large number of failed attempts to log into the system, register and make calls affects the performance of the system. Such behavior could cause denial of service, making the services unavailable for legitimate users.

**Source: http://www.theregister.co.uk/*

7 arrested for SIM Box fraud in Ghana causing losses of over USD 21 million

Continuing their efforts to clamp down on the operations of SIM box fraudsters, the Anti-Telecom Fraud Task Force of Ghana has arrested another gang of fraudsters for allegedly diverting international calls through SIM box machines mounted in their premises.

The operations by the gang are said to have resulted in a USD 21 million revenue loss to the state. A total of 2,395 SIM cards of all major operators in the country were retrieved. Other items found by the police included SIM box machines, laptops, generating sets, mobile phones, Internet routers, and an internal antenna. With these systems, the suspects enabled the calls to bypass the national gateway, hence depriving the government of revenue from such calls.

**Source: http://pulse.com.gh/*

Italian privacy body fines dealers €500,000 for SIM fraud

Garante Privacy, Italy's data protection authority, has fined 14 dealers a total of over €500,000 for using personal data of 142 people to issue SIM cards without their knowledge. The SIM cards were subsequently used for criminal activities and the fines were imposed after a complex investigation by Italy's financial police, said the watchdog. The investigation remains ongoing.

**Source: http://www.telecompaper.com/*

For all previous fraud alerts click on the following link: http://www.subex.com/fraud-alerts To follow active discussions on various topics log on to or subscribe to: Telecom Fraud Professional Group LinkedIn, @ SubexTweets and Subex Blog.

Write to us at info@subex.com to know more about dealing with telecom frauds.