

# Telecom Fraud Alerts

January - March 2015

## Two of FBI's 'Cyber Most Wanted' arrested in Pakistan for PBX Fraud

Two individuals named on the Federal Bureau of Investigation's most-wanted list of suspected cyber criminals have been captured by authorities in their native Pakistan.

Authorities in the United States say that the hackers were involved in an international crime ring that scammed telecommunication companies out of an estimated \$50 million between in the last few years.

The hackers targeted PBX (Private Branch Exchange) telephone systems of corporations and placed calls to those systems in an attempt to identify telephone extensions that are not in use. Once an unused extension was identified, hackers illegally reprogrammed the telephone system. The hacked telephone system could then be used by the hackers and others to make long distance telephone calls that are charged back to the victim corporation, creating virtually free telephone lines through which they could make calls. Using these compromised lines, calls were made to premium rate lines which were operated by the hackers.

As a result of the conspiracy, telephone companies and the hacked entities lost tens of millions of dollars due to more than 13 million minutes of telephone calls over 4,800 hacked PBX systems.

\*Source: <http://rt.com/usa>, February 2015

## Serbian police cracks down on illegal SIM box scheme

Serbia's Interior Ministry, in cooperation with the Special Department for Cyber Crime of the Prosecutor's Office and the Ministry of the Interior of Macedonia, have identified several suspects in Belgrade and Gostivar illegally using telecommunications and computer equipment, called SIM boxes, reports Politika. The suspects are accused of bypassing international telecommunication services using VoIP technology on unregistered pre-paid mobile phone connections of domestic mobile operators.

By illegally redirecting telephone traffic to Serbian citizens living in the EU, they allowed low-cost calls with interlocutors in Serbia. More than 40,000 SIM cards were found in Macedonia of mobile operators from Serbia, Croatia, Slovenia, Albania, Bosnia and Herzegovina, which were used to further calls to mobile subscribers, so that international VoIP traffic was realised as a national call from a local SIM card.

\*Source: <http://www.telecompaper.com>, March 2015

## New Whatsapp Wangiri Fraud hits South Africa

A new WhatsApp Wangiri fraud campaign has emerged in South Africa where local WhatsApp users are urged to call an international number which incurs significant costs.

Wangiri is a type of phone fraud where the perpetrator dials random mobile numbers and then hangs up after one ring. A missed call then shows on the recipient's phone. Users then call back believing it was a legitimate call (or are simply curious), but unbeknown to them the numbers are premium rated. Users may also be spammed with automated advertising messages when they return these calls.

In the WhatsApp-based version of Wangiri fraud, users receive a WhatsApp message with a contact attachment. However, the number in the contact is different from the number the message originated from. When the victim calls the provided number, he/she is charged at a premium rate.

\*Source: <http://mybroadband.co.za>, January 2015

## Uganda probes possible USD 144 m telecom fraud

Uganda's Financial Intelligence Authority is investigating suspected fraud in the telecommunications sector, which could amount to USD 144 million in lost revenue.

The fraudsters are reportedly using data codes to illegally terminate international mobile phone traffic (grey traffic) into local networks disguised as local traffic. The traffic that goes through official international gateways is instead delivered through Sim-Boxes (racks containing hundreds of local numbers) and is received as local traffic. The fraudsters end up paying only an eighth of the money they should have paid to the main voice operators in interconnection fees.

The Financial Intelligence Authority issued an alert to the Uganda Communications Commission about the loss of up to USD 144 million over the last three years. Authorities also fear that the money generated through the fraud could be used to compromise national security.

\*Source: <http://www.telecompaper.com>, March 2015

## SIM Box fraudsters busted in USD 100 m fraud

Ghanaian anti-fraud agencies have arrested local residents and foreigners engaged in SIM Box fraud, diverting more than \$100 million from the coffers of the West African country.

Ghana has been grappling with the menace of SIM box fraud and between October 2010 and August 2014, 13 SIM box fraud cases were recorded were 13 and 17 suspects, both Ghanaian and foreign – including an Italian – were arrested. The fraudsters allegedly route calls from overseas through the internet and terminate them through local SIM cards fitted into SIM boxes.

In the past, the crime was limited to the capital Accra, but signals received on the ground and the arrests made in various parts of the country confirm that the activities had become widespread.

\*Source: <http://www.theafricareport.com>, January 2015

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

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

Get in touch with our experts to know more about dealing with telecom frauds.