Subex Telecom Fraud Alerts

June 2010

PRS Scams with video files

There are new tricks being developed to elicit people to dial a PRS line and defraud them. In one of the scenarios, someone downloads a video file from web or P2P sharing software. When the file is played, the following message appears:

"This video can only be played in <Some Player>, Visit <some URL> to download and play it.

When the software is run, it locates the user, directs them to a telephone hotline appropriate to their country and instructs them to call via cell-phone to 'unlock' the software free of charge. The call leads to PRS numbers, costing the user money.

End user awareness is the best method of preventing such frauds.

3D Anti-Terrorist continues to flourish, now with Antarctica numbers

Today's hi tech fraudsters have started using telephone numbers in the Antarctic to elicit cash from victims. As previously reported, a malicious version of the 3D Anti-Terrorist mobile game contains hidden code which dials expensive long distance numbers, making the phone silently ring numbers in the Antarctic number block (prefix +88234). This is occurring despite there being relatively few phones and phone numbers in use in Antarctica.

Calls made to Antarctica typically cost about 5 euros (£4.25) per minute from a mobile. The rogue game was discovered in April but is still on the increase, as it has been uploaded to many sites offering applications for Windows mobiles. Premium rate and international numbers are a good target, as hitting a small number of victims quickly generates a lot of cash for the fraudsters. Research by Kasperksy Labs suggests that the mobile threats have seen more than 200% growth in the past three years.

Operators are advised to educate and alert their customers of any such scams.

**Source: BBC News, May 2010*

Telecom DDoS used to conceal cyber crime

A new scheme of cyber crime using telecommunication distributed denial of service (DDoS) has been detected recently by the FBI. According to the FBI, the victims are being bombarded with unsolicited and mysterious phone calls to their mobiles and landlines in order to distract victims from the attempts made by the criminals to empty their bank and trading accounts. According to the telecom companies working with the FBI, these attacks, known as telephony denial-of–service (TDOS), have seen a huge spike recently.

The crooks use automated systems to place calls to prospective victims, and while the victim is distracted by the call, the criminals transfer funds from the victim's bank or trading accounts. As a result, financial institutions that detect the fraud are unable to get in touch with the victim until it is too late. The first such incident occurred in November 2009, when a leading telecom operator in the US saw an increase in this activity targeting its customers across the country.

Although unsolicited telephone calls may not always be representative of fraud, the FBI has advised operators to warn its customers of such an attack. The customers should be advised to report such TDOS attack or any other fraud and should implement strong security for all their financial accounts.

**Source: The New New Internet, May 2010*

Call Barring to curb roaming IRSF

Recent discussions with operators and operator groups have highlighted considerable differences in the scale and nature of IRSF across different operators. It also seems that some of the standardized roaming bar capabilities that can help reduce roaming IRSF are relatively under-utilized by operators. These capabilities include restricting outbound roaming calls to in-country and/or home country only, and use of the more recent OBOPRE/I (Operator Barring of Premium Rate Entertainment / Information).

If such bars are not already being employed, it is recommended that mobile operators consider reviewing their international roaming polices with this in mind.

Note: For OBOPRE/I to work correctly, the roaming partner must configure their national premium rate number ranges in their MSCs. This is not always the case in practice.

New phone scam – Kidnapping threats of mobile phone users

A phone scam has emerged in parts of Central & Latin America, North America and Asia Pacific. The modus operandi of this is as follows:

- Mobile phone users get a call from someone claiming to work for their service provider, asking them to switch off their phones for 2 hours for an upgrade to 3G to take place.
- Once the unsuspecting user switches off her phone, the perpetrators call up her friends / family, claim that the user has been kidnapped, and ask for large sums of money to be transferred to their bank accounts as ransom. In many cases, the friends / family members of the user have even thought they heard the 'user's voice' calling out for help during these ransom calls.

Service providers are using different methods to tackle these problems, such as cell site origination; pattern of usage (e.g. dialed numbers are in sequence); high number of calls without high minutes of usage (usually short calls to numerous different numbers); etc. At the same time, service providers in susceptible areas could alert their users of the possibility and modus operandi of such scams.

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