

# Subex Telecom Fraud Alerts

April 2010

## New Zealand firms – the latest victims of PBX hacking

New Zealand businesses have been targeted by overseas phone system hackers who are running up large bills on the victims' accounts. The fraudsters hacked into office phones and used them to call an 0900 number in Somalia.

The scam was detected when the operator noticed dozens of calls being made to a Somalian number in the early hours of the morning. The operator's fraud team spotted the unusual activity and put a toll bar on the company's line. The amount of money collected by this scam is still unknown. In this instance, every call to the 0900 number resulted in money being added to the number owner's account, and the victims were also hit by international toll charges.

Telecom operators in New Zealand have warned their customers repeatedly to ensure they don't become vulnerable to these scams. The hackers could be operating from anywhere in the world and have a number of ways to hack into a badly managed PABX. They can exploit the voicemail feature of office phones that lets staff call from a remote location, enter a PIN and check messages. Or they can breach codes used by engineers to carry out system maintenance. Telecom operators have advised PABX owners to introduce PIN and password policies to foil hackers. It is the responsibility of PABX owners to ensure it is secure as the PABX is directly linked to their wallet through their phone account.

*\*Source: The New Zealand Herald, April 2010*

## Emergence of Malicious Mobile Trojans to call PRS numbers

A new game called 3D Antiterrorist has been appearing on a number of international freeware sites offering downloads for the Windows Mobile Smartphone. As well as the game itself, the 1.5 MB archive contains the file reg.exe - a Trojan that automatically calls premium rate international numbers. The malicious program has been detected by Kaspersky Labs as Trojan.WinCE.Terdial.a.

After the antiterrorist3d.cab installation file is launched, the game is installed in Program Files, while the malicious file reg.exe (5632 bytes) is copied to the system directory under the name smart32.exe.

A closer inspection of the malicious program's code reveals that:

- it was created by Russian-speaking virus writers;
- calls are made to 6 different premium-rate numbers every 50 seconds;
- it uses the CeRunAppAtTime function to self-launch, and it launches at night when the Smartphone owner is most likely to be oblivious to the calls.

The list of numbers called includes:

- +882\*\*\*\*\*7 - International Networks
- +1767\*\*\*\*\*1 - Dominican Republic
- +882\*\*\*\*\*4 - International Networks
- +252\*\*\*\*\*1 - Somalia
- +239\*\*\*\*\*1 - Sao Tome and Principe
- +881\*\*\*\*\*3 - Global Mobile Satellite System

*\*Source: securelist.com*

## A Variation on Mailbox Hacking – CLI Spoofing

In our February 2010 Fraud Alert, we discussed the impact of CLI Spoofing. In many CLI spoofing attacks the attackers typically use VoIP service and change their presented Caller Line Identification (CLI) to the number of the targeted victim. There are many commercially available spoofing services on the market such as: <http://www.telespoof.com> or <http://www.bluffmycall.com>. CLI spoofing is commonly used to gain anonymity, or to have services billed against another account. Recently though, there have been instances of CLI spoofing being used for mailbox hacking.

In networks where mailbox access is possible from external networks, and where access control is based on presented CLI, a call by the attacker will be directed to the targeted mailbox. Accessing deposited mail, changing mailbox settings, and possibly setting up outbound calls may then be possible.

Solutions include: not using the presented CLI for mailbox access control, disabling of dialing voicemail except from within home network (via a short code), or mandating the use of PIN codes and a strong PIN security policy.

*\*Source: GSMA FF*