TELESHIELD™

CASE STUDY 1

International Premium Rate Number (IPRN) Database

Introduction

Between November and January, a small Telecom Carrier in the Asia Pacific region was having persistent IRSF attacks on their network, primarily using hacked PBXs as the calling enabler. Each month, the fraud attack would start around the second week of the month, continue for about 20 days, then stop until the next month, when it would start again.

The victim Carrier requested assistance to see if it was possible to both confirm that these attacks were International Revenue Share Fraud, and to advise them if the IPRN database could have prevented this attack, and any further IRSF attacks they may suffer.

DETAILS OF THE FRAUD

The fraud incident evaluated was the attack that occurred in January. Details of this fraud were:

- This attack occurred between the 6th and 29th January.
- There were 4,400 calls made to 1002 unique numbers in 55 Countries.
- The total duration of these calls was 47,869 minutes (797 hours), an average of 34 hours per day.

INTERNATIONAL REVENUE SHARE FRAUD

- Analysing the numbers called during this IRSF attack identified 367 numbers with a 100% match to IPRN database numbers and another 231 partial matches to the last digit. This represents a 59.67% success rate, with 598 of the 1002 unique numbers being identified by using the IPRN database.
- Matching these identified numbers against the calls made found that 756 of the calls made were to numbers that were a 100% match to the IPRN database while another 1281 calls were a partial match to the last digit. This represents a 52.43% success rate, with 2037 of the 4,400 calls identified.

Could the IPRN database have prevented this fraud?

Absolutely. The 4th and 5th calls made during this fraud were to partial matching numbers in the IPRN database and the 7th and 8th calls were to 100% matching numbers. Of the first 50 calls made of the 4,400, 42 were made to IPRN numbers and would have generated fraud alerts had the IPRN database been in place on this network. The fraud certainly would have been discovered and shut down on day one of the fraud, preventing it from continuing for another 23 days before being discovered.

CONCLUSION

This is typical of the results we are receiving from use of the IPRN database and it is not unusual when we are carrying out this type of analysis on historical cases to find 60 or 70% matches with numbers in the IPRN database.

tmt id
tmtid.com
+44 (0) 207 193 5161