IRSF: a Billion $ Fraud Abusing International Premium Rate Numbers

Merve Sahin, Aurélien Francillon
EURECOM
Sophia Antipolis, France
merve.sahin, aurelien.francillon@eurecom.fr

***Abstract*—Premium phone numbers are often abused by malicious parties (e.g., via various phone scams, mobile malware) as a way to obtain monetary benefit. This benefit comes from the 'revenue share' mechanism that enables the owner of the premium rate number to receive some part of the call revenue for each minute of the call traffic generated towards this number.**

This work focuses on International Revenue Share Fraud (IRSF), which abuses high cost international destinations as so-called *International Premium Rate Numbers (IPRN)*. IRSF often involves multiple parties who collect and share the call revenue, and is usually combined with other fraud schemes to generate call traffic without payment.

We aim to explore the IRSF ecosystem by analyzing the online IPRN resellers and their test portals frequently used by the fraudsters: We present our observations on the more than 517K international premium rate test numbers collected from such test portals. Finally, we present our findings from a telephony honeypot that observes IRSF attempts towards an unused phone number range (i.e., *a phone number gray space*).

I. Introduction

International Revenue Share Fraud (IRSF) costs telecom operators $6.10B a year (roughly 20% of estimated communication fraud) [4]. IRSF can affect all users of the telephone network, both individuals (fixed lines, prepaid and postpaid mobile subscribers) and the enterprise phone systems. In IRSF, fraudsters can generate the illegitimate calls in various ways, such as using fraudulently obtained SIM cards [8], tricking fixed/mobile line users to call back the premium numbers (e.g., one-ring or 'Wangiri' scam) [5], compromising the phone system (PBX) of a company to initiate calls [6], or via mobile malware that stealthily calls the premium numbers [2].

Such illegitimate calls are usually hijacked during their transit, and re-directed to so-called 'premium' services. In this case, the calls will not reach the actual termination operator, who is the legitimate owner of the phone numbers. Because of the opacity of international phone call routing, it is often impossible to know the real route that a call takes, and therefore, to identify the fraudulent transit operator [7].

On the other hand, fraudsters use openly advertised test numbers before generating call traffic, to identify if they can obtain the cash back (calls can be blocked to this destination or not all routes leads to a hijack). A simple online search for *international premium rate numbers* reveals many websites advertising them, and promising fast, easy money pay-back guarantee for the call traffic generated to these numbers. Some of the websites also provide easy setup for ready-to-use IVRs (such as audio books, weather services) that can be used for the premium rate service.

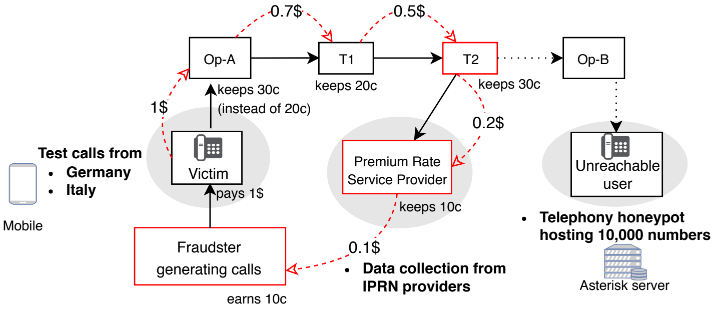

Fig. 1. Summary of experiments on International Revenue Share Fraud.

In addition, such websites often provide web interfaces for testing purposes: they publish a set of 'test numbers', so that the fraudsters can check if the calls they generate are actually routed through the involved fraudulent transit operator (consider the 'Transit operator T2' in Figure 1), as routing through another route will not generate revenue. Such test numbers may actually belong to an unallocated or unused number range (i.e., a *phone number gray space*). Otherwise, if the call does not go through the fraudulent operator (i.e., if a legitimate route is taken instead of the fraudulent route), test calls may ring the phones of genuine users. The test panels also keep the CDR logs for the calls that are initiated to the test numbers. Fraudsters can view the call records in real time, to check if the current call they are making has reached the premium rate provider. These test calls are usually initiated from a phone system that will soon become a victim of IRSF (e.g., a compromised PBX, a stolen mobile phone).

In this work, we present our observations on IRSF ecosystem using the data we collected from the test panels of various online IPRN providers, and a telephony honeypot located in a small European country (Figure 1).

II. Analyzing IRSF via Online IPRN Providers

From January'16 to April'18, we collected 517,319 unique IPRN test numbers from 10 websites advertising IPRNs. Moreover, we used a commercial numbering plan database[1] to extract further information on the test numbers and verify their validity.

TABLE I
VALIDITY OF IPRN TEST NUMBERS

	Valid length	Invalid length	Total
Valid range	73.1%	10.9%	84.0%
Unallocated range	5.8%	10.2%	16.0%
Total	78.9%	21.1%	100%

A. Analyzing test IPRNs

Overall coverage. Our dataset includes test numbers from 236 countries[1] and 869 operators[2]. This shows that IRSF can target a large variety of countries, with varying call termination costs. Indeed, the whitepaper by TransNexus [3] analyzes payout rates from 193 countries and mentions that the fraudster's benefit can be as low as $0.00013 per minute, which strongly incites fraudsters to massively abuse phone systems to generate revenue.

Validity. In Table I, we present the validity of the test numbers, classified by the validity of the number range and number length. Number range validity checks if the number belongs to an allocated range defined in the numbering plan database Overall, 73.1% of the numbers belong to a valid number range and have a valid length according to the numbering plan database we use. The remaining 26.9% either have an invalid length, or belong to an unallocated number range, or both.

Number type. Next, we look at the number type information for these test numbers. Our numbering plan database specifies a number type for each allocated number range. However, for the 16% of the test numbers which do not match an allocated number range, number type information is not available. We found that, while all types of phone numbers (landlines, satellite numbers) can be abused as IPRNs, mobile number ranges are the most frequently abused (57.4% of collected IPRNs).

Dispersion of numbers.

For the top 5 countries with the largest number of advertised test numbers, Figure 2 shows the number of collected test numbers, and unique number ranges when the last 1 and 2 digits are ignored. As we can see from this figure, the quantity of test numbers are not always an indication of the *dispersion* of abused number ranges in that country. For instance, although Latvia has the highest count of test numbers, these numbers belong to a smaller set of number ranges, especially when compared to Cuba.

In conclusion, our analysis shows that there is a large variety of number ranges that can potentially be abused for IRSF: Both fixed and mobile numbers, invalid length numbers, unallocated number ranges, and number ranges of various types of operators are being abused as IPRNs.

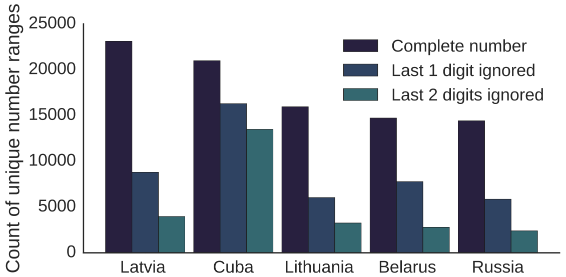

Fig. 2. Top 5 countries having IPRN numbers advertised.

III. A TELEPHONY HONEYPOT OBSERVING IRSF ATTEMPTS

Our honeypot consists of 10,000 phone numbers that are essentially reserved for quality control and testing purposes, and thus, not supposed receive any calls.

During the 2-year period, our honeypot received 259 international calls from 77 different countries. However, between 11th to 16th of January'17, we observed an unusual call traffic: over 120 calls in 5 days. In addition, we periodically generate test calls to the honeypot numbers from customized Android handsets located in Italy and Germany. Starting from the 6th of January'17 (12pm) to the 7th of January'17 (5am), 30 test calls originating from Germany were answered and billed for 1,5 minutes on average. However, these calls were not even received by the honeypot.

This incident is a strong evidence that our honeypot number range was advertised as an IRSF destination during this time period, and it attracted a lot of call traffic. Although the 117 calls we observe at the honeypot were failed IRSF attempts, the hijacking of the number range was indeed successful on the test calls that we originated from Germany.

IV. CONCLUSION

In this work, we study the long-standing, yet unsolved problem of International Revenue Share Fraud (IRSF). We first analyzed the data we collected from online IPRN providers to understand how they operate and how they abuse international phone numbers. We then present an example case of an hijacked phone number range, using a telephony honeypot. In the future, we aim to utilize these data sources to develop fraud detection mechanisms for IRSF.

REFERENCES

[1] National Numbering Plans Collection. http://www.numplans.com/numbering-plans/.

[2] You will be billed $90,000 for this call 3: F-secure discloses mobile app virus attacks. Privacy-PC.com news, March 2012.

[3] International premium rate number market, 2015.

[4] CFCA. 2017 Global Fraud Loss Survey. http://cfca.org/fraudlosssurvey.

[5] C. McDaid. Ireland's Call , Careful Now. www.adaptivemobile.com, October 2017.

[6] N. Perlrothoct. Phone hackers dial and redial to steal billions. www.nytimes.com, October 2014.

[7] M. Sahin, A. Francillon, P. Gupta, and M. Ahamad. Sok: Fraud in telephony networks. EuroS&P'17. IEEE, April 2017.

[8] L. Watson. Five men jailed for 4.5m worldwide premium phone number scam. http://www.dailymail.co.uk, October 2011.

[1] This number also covers the territories and satellite services that have their own number ranges. Our numbering plans includes 247 such ranges.

[2] Note that operator information is only available for mobile numbers. Our numbering plan includes 1522 different mobile operators (including MVNOs).