Case Study: Wangiri Fraud Prevention

Onyx FMS Implementation for Bitė Group

Background

Bitė Group is a leading telecommunications and media group in Lithuania, Latvia, and Estonia. Among other subsidiaries, Bitė Group controls two mobile network operators: Bitė Lietuva in Lithuania (around 1M subscribers) and Bite Latvija in Latvia (around 0.5M subscribers).

Elitnet has been providing Bitė with various telecommunications software solutions since 2005, including telecom application servers, value-added services, and data analytics applications.

Challenge

According to Communications Fraud Control Association's (CFCA) global Fraud Loss Survey, Wangiri fraud, also known as callback fraud, has entered the top five most prevalent fraud types in 2019 and is quickly "becoming a major worldwide issue". Wangiri fraud involves execution of short-duration calls from high-rate countries and phone numbers with the intention to initiate a callback from the subscriber.

Bitė has been facing increased Wangiri fraud activity, resulting in subscriber complaints and additional expenses to compensate defrauded subscribers. Some major Wangiri attacks faced by all local mobile network operators were widely described in the local media, prompting all operators to ensure that their subscribers are completely protected from this type of fraud.

Classic Wangiri attacks used to consist of a large number of calls from a small amount of different numbers, making them relatively easy to detect. However, modern-day Wangiri attacks consist of a large quantity of geographically diverse, non-repeating numbers (up to 40,000 per attack) with a very small amount of calls from each of them carried out in just a few hours.

This meant that the legacy Wangiri detection methods based on attacking number databases and rules were not able to efficiently detect the new type of attacks or detected them after the attack when the damage has already been done.

TOP 5

Most prevalent fraud type based on CFCA Fraud Loss Survey

$1.82B

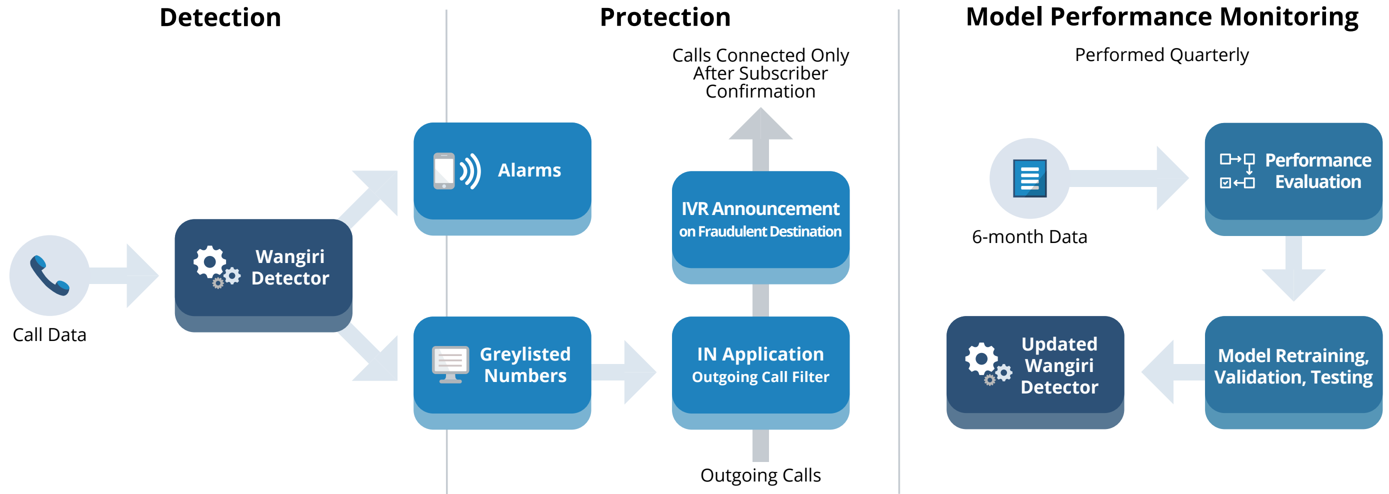
Estimated annual global loss due to Wangiri attacks

Consequently, Bitė was in the market for a solution which would focus on the following key points:

- Detect Wangiri attacks as quickly as possible and minimize the fraud window during which most of the losses occur.
- Ensure that instead of blocking a potentially fraudulent direction, subscribers are warned that they are calling to a high-risk number before connecting the call.
- Identify numbers used for Wangiri fraud and store them in an internal grey list used to warn subscribers about possible fraud.
- Constantly monitor the situation in the network and adapt to changing fraud attack patterns as new types of attacks take place.

Approach

To detect and prevent Wangiri and other fraud types, Elitnet proposed to provide Bitė with **Onyx Fraud Management System** (Onyx FMS). Onyx ensures hybrid real-time fraud prevention by collecting data from the network, processing and analyzing it using both rules and ML methods, and using the results to provide statistics and reports, send alarms and notifications, or prompt other network components to take necessary actions.


Detection
Protection
Model Performance Monitoring
Performed Quarterly
Calls Connected Only After Subscriber Confirmation
Alarms
IVR Announcement on Fraudulent Destination
Call Data
Wangiri Detector
Greylisted Numbers
IN Application Outgoing Call Filter
Outgoing Calls
6-month Data
Performance Evaluation
Model Retraining, Validation, Testing
Updated Wangiri Detector

Onyx's Wangiri Detector component is based on a residual neural network, a state-of-the-art deep learning model that is trained to understand the operator's network instead of specific attacks. The model learns the patterns of the traffic flowing through the network to become capable to identify any Wangiri-related abnormalities.

After detecting a Wangiri attack, Onyx ensures that any subscribers calling back to numbers associated with the attack are warned before connecting the call. Later on, this IVR warning may also be played to all subscribers calling to any numbers previously associated with a Wangiri attack.

Onyx uses historical data, pricing levels, and current traffic information to differentiate attacks according to their probability. Low-probability attacks can be analyzed and evaluated to quickly react to any changes in Wangiri fraud manifestations, ensuring detection and prevention of new types of attacks.

Results

The following results were achieved by Onyx FMS when detecting Wangiri fraud attacks:

Individual call level

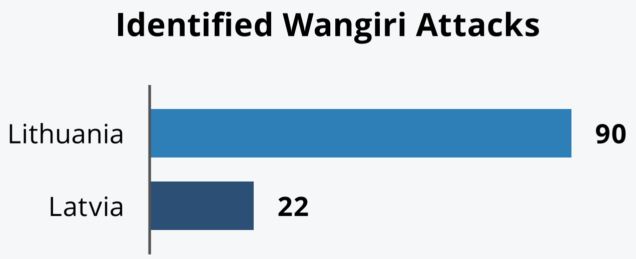
- **97%** recall
- **92%** precision
- **94%** F1 score

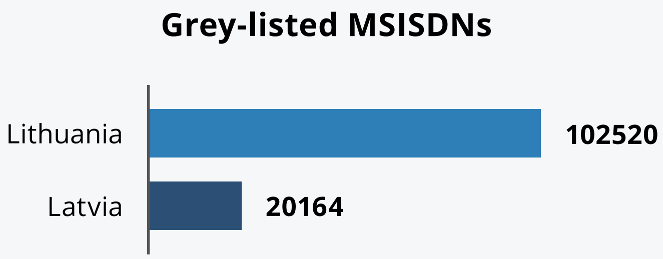
Attack level

- **99%** recall
- **100%** precision
- **100%** F1 score

Attacks are **identified within the first 20 fraudulent calls**, which means that it usually takes only a few minutes or even seconds to identify and block the attack. Even though a few individual calls may go unnoticed during an attack, Onyx FMS has an impeccable record of detecting and successfully blocking attacks as a whole.

During the first two months after implementing Onyx for both Lithuanian and Latvian Bitė operators and training the ML model (Apr-Jul 2021), the system gathered the following statistics:





When Wangiri attacks take place, the implemented IVR alert system warns the subscribers about suspicious call directions, allowing them to avoid bill shock and resulting in a positive customer experience.

This showcases Bitė's concern for protection of its subscribers and has resulted in numerous cases of positive customer feedback in social media.

> *In just a few months, Onyx made Bitė a much less attractive option for Wangiri fraudsters, as we are detecting and blocking even the new type Wangiri attacks in a matter of a few minutes. All of this was achieved without any negative experience for our subscribers.*
>
> *Both Wangiri and other fraud prevention modules implemented with Onyx FMS have provided us with significant improvements in fraud detection, analysis, and prevention.*
>
> - Indrė Bobraitienė, RA Manager, Bitė Group

> *In addition to fraud detection and prevention, Onyx is a very valuable reporting system for business intelligence and revenue assurance. It also opens up new possibilities for device classification, predictive maintenance, and other promising solutions.*
>
> - Jonas Milerius, Head of Roaming, Interconnect & Fraud, Bitė Group

ELIT NET

www.elitnet.eu
info@elitnet.eu
+370 37 352706

UAB Elitnet
Pasiles 102, LT 51314
Kaunas, Lithuania