MOBILEUM

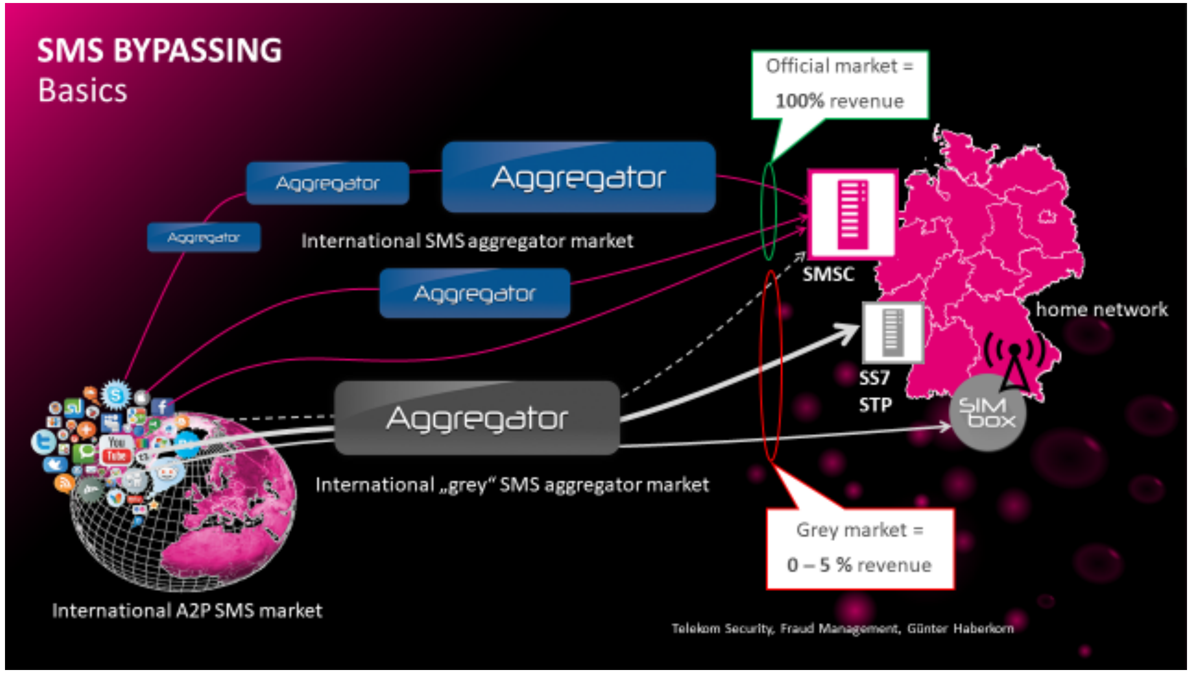
# SMS Firewall

© 2019 Mobileum, Inc. All rights reserved. Confidential and Proprietary Information of Mobileum, Inc.

# SMS Firewall

- Identifies A2P sender (grey route)
  - Alphanumeric
  - Short code
  - Valid for sending country
- SRI correlates to FSM source
- AA19 checks
- MO spoofing check (location)
- Matches regular expressions on content
  - A2P
  - Spam
  - Including binary strings, iPhone attack character
- Identifies repeated similar text
- Guides user to create new regexp

- National and International traffic
  - Grey route may be via national partner
  - May be SIM box in national partner
  - Local NIF processes national traffic

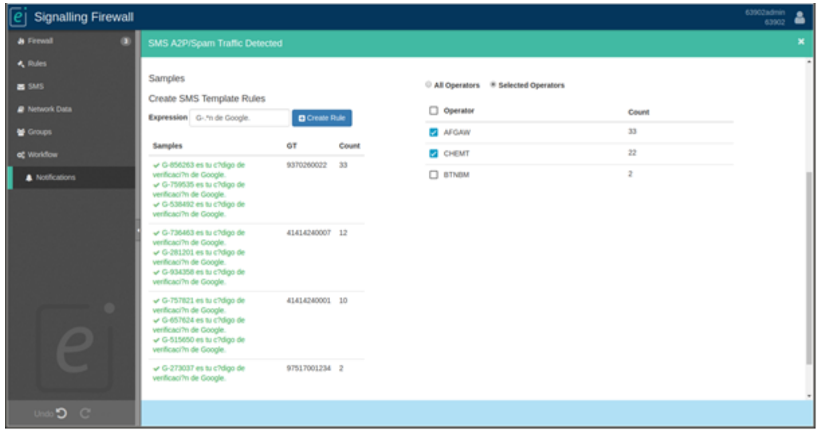

SMS BYPASSING
Basics
Official market =
100% revenue
Aggregator
Aggregator
Aggregator
International SMS aggregator market
Aggregator
SMSC
home network
SS7
STP
SIM box
Aggregator
International „grey“ SMS aggregator market
Grey market =
0 – 5 % revenue
International A2P SMS market
Telekom Security, Fraud Management, Günter Haberkorn

© 2019 Mobileum, Inc. All rights reserved. Confidential and Proprietary Information of Mobileum, Inc.

# SMS Firewall

## Identifying new spam

- Updated from multiple safe URL databases
- Two separate algorithms identify potential spam with examples and source
- Simple options presented in workflow to block source or create regular expression
- Rule actions and exceptions can then be defined



SMS A2P/Spam Traffic Detected

Samples

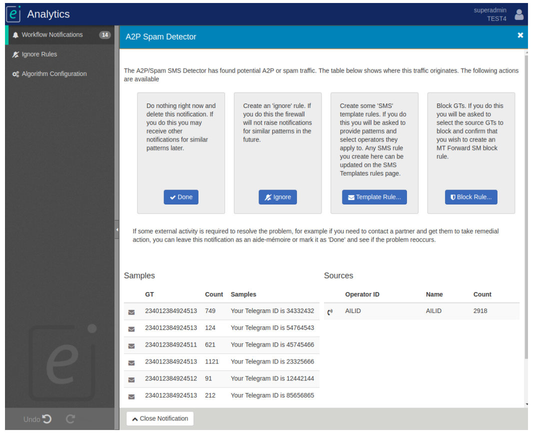
Create SMS Template Rules

**Expression** G-.*n de Google. [Create Rule]

| Samples | GT | Count |
|---|---|---|
| ✓ G-856263 es tu c?digo de verificaci?n de Google.<br>✓ G-759535 es tu c?digo de verificaci?n de Google.<br>✓ G-538492 es tu c?digo de verificaci?n de Google. | 9370260022 | 33 |
| ✓ G-736463 es tu c?digo de verificaci?n de Google.<br>✓ G-281201 es tu c?digo de verificaci?n de Google.<br>✓ G-934358 es tu c?digo de verificaci?n de Google. | 41414240007 | 12 |
| ✓ G-757821 es tu c?digo de verificaci?n de Google.<br>✓ G-657624 es tu c?digo de verificaci?n de Google.<br>✓ G-515650 es tu c?digo de verificaci?n de Google. | 41414240001 | 10 |
| ✓ G-273037 es tu c?digo de verificaci?n de Google. | 97517001234 | 2 |

○ All Operators ● Selected Operators

| □ Operator | Count |
|---|---|
| ☑ AFGAW | 33 |
| ☑ CHEMT | 22 |
| □ BTNBM | 2 |



A2P Spam Detector

The A2P/Spam SMS Detector has found potential A2P or spam traffic. The table below shows where this traffic originates. The following actions are available

Do nothing right now and delete this notification. If you do this you may receive other notifications for similar patterns later. [✓ Done]

Create an 'ignore' rule. If you do this the firewall will not raise notifications for similar patterns in the future. [Ignore]

Create some 'SMS' template rules. If you do this you will be asked to provide patterns and select operators they apply to. Any SMS rule you create here can be updated on the SMS Templates rules page. [Template Rule...]

Block GTs. If you do this you will be asked to select the source GTs to block and confirm that you wish to create an MT Forward SM block rule. [Block Rule...]

If some external activity is required to resolve the problem, for example if you need to contact a partner and get them to take remedial action, you can leave this notification as an aide-mémoire or mark it as 'Done' and see if the problem reoccurs.

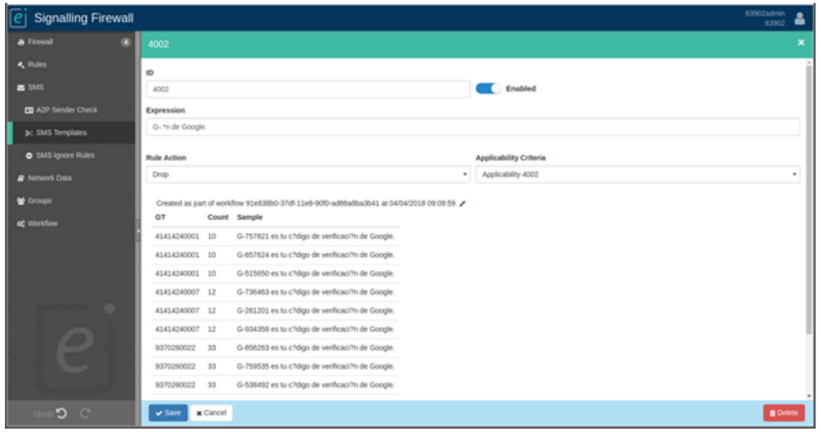
Samples

| GT | Count | Samples |
|---|---|---|
| 234012384924513 | 749 | Your Telegram ID is 34332432 |
| 234012384924513 | 124 | Your Telegram ID is 54764543 |
| 234012384924511 | 621 | Your Telegram ID is 45745466 |
| 234012384924513 | 1121 | Your Telegram ID is 23325666 |
| 234012384924512 | 91 | Your Telegram ID is 12442144 |
| 234012384924513 | 212 | Your Telegram ID is 85656865 |

Sources

| Operator ID | Name | Count |
|---|---|---|
| AILID | AILID | 2918 |

Close Notification



4002

**ID** 4002 Enabled

**Expression** G-.*n de Google.

**Rule Action** Drop

**Applicability Criteria** Applicability 4002

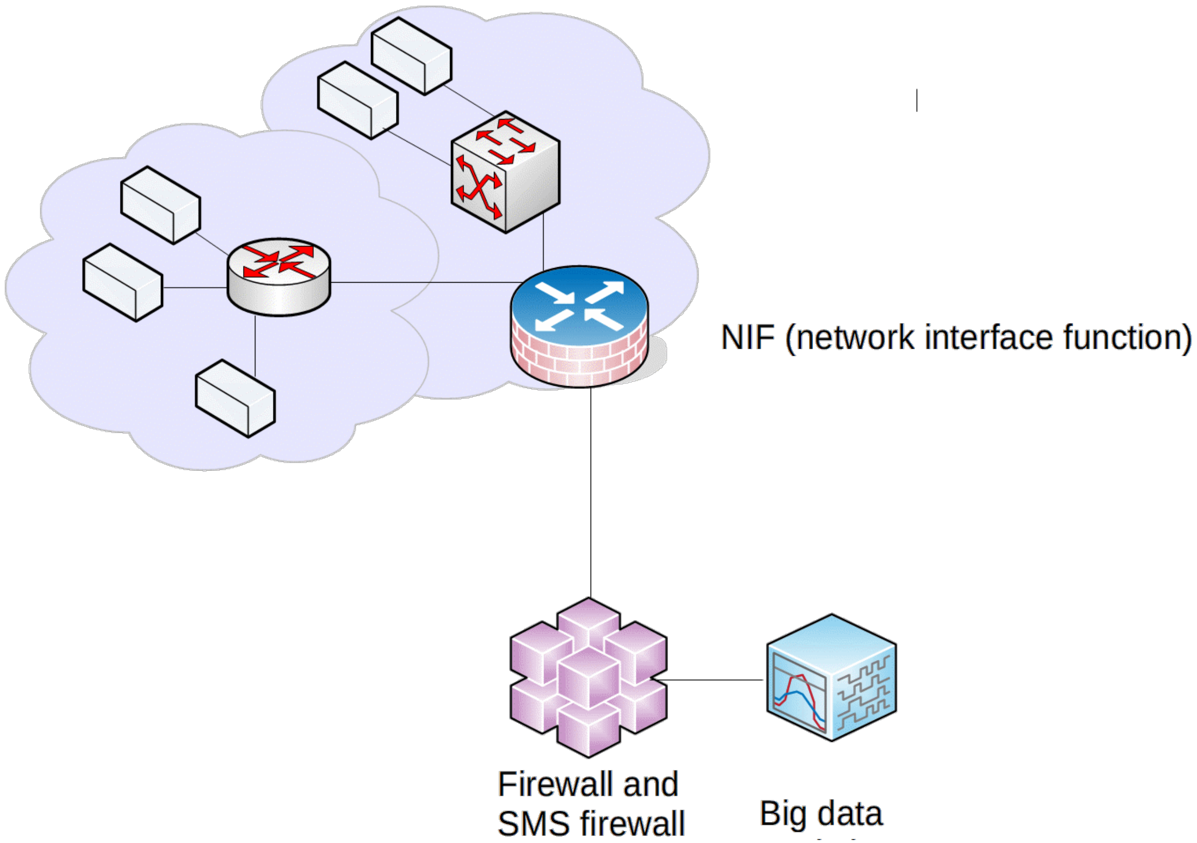
Created as part of workflow 91e838b0-37df-11e8-90f0-ad66a8ba3b41 at 04/04/2018 09:09:59

| GT | Count | Sample |
|---|---|---|
| 41414240001 | 10 | G-757821 es tu c?digo de verificaci?n de Google. |
| 41414240001 | 10 | G-657624 es tu c?digo de verificaci?n de Google. |
| 41414240001 | 10 | G-515650 es tu c?digo de verificaci?n de Google. |
| 41414240007 | 12 | G-736463 es tu c?digo de verificaci?n de Google. |
| 41414240007 | 12 | G-281201 es tu c?digo de verificaci?n de Google. |
| 41414240007 | 12 | G-934358 es tu c?digo de verificaci?n de Google. |
| 9370260022 | 33 | G-856263 es tu c?digo de verificaci?n de Google. |
| 9370260022 | 33 | G-759535 es tu c?digo de verificaci?n de Google. |
| 9370260022 | 33 | G-538492 es tu c?digo de verificaci?n de Google. |

© 2019 Mobileum, Inc. All rights reserved. Confidential and Proprietary Information of Mobileum, Inc.

# Advanced analytics - optional module

- Complements algorithms in SMS FW
  - Optional module
- Identifies spam and A2P including “zero day” attacks
  - Intent keywords to create code string (e.g. M (money) for $, USD, 4 etc)
  - Code string signature used for big data analysis
  - Supervised and unsupervised learning identifies A2P / spam as outliers
  - Provides confidence level
- Automates blocking based on confidence metrics



© 2019 Mobileum, Inc. All rights reserved. Confidential and Proprietary Information of Mobileum, Inc.

MOBILEUM

# Thank You

© 2019 Mobileum, Inc. All rights reserved. Confidential and Proprietary Information of Mobileum, Inc.

MOBILEUM

# Back Up

© 2019 Mobileum, Inc. All rights reserved. Confidential and Proprietary Information of Mobileum, Inc.

# Keyword Dictionary

- Incoming SMS text is converted into a sequence of keywords
  - Stop words are removed before keyword checks, Jaccard algorithm used for approximate matching
- Keywords indicate intent
  - URL **(U)**: Word having http, https, www, .com
  - Money **(M)**: Currency abbreviations like $, AED etc.
  - Corporate (**C**): Common company names e.g. facebook, uber etc.
  - Names (**A**): Typical names (country specific)
  - Number (**N**): Any number
  - Spam (**S**): typical spam words like sweepstake, lottery, bonus etc.
  - Profanity (**P**): cuss words
  - Emotion (**E**): depicting emotions like love, joy, surprise etc.
  - OTP/Security (**O**): words indicating password of otp content
  - HAM Common (**D**): commonly used words in HAM messages (can be present in SPAM/A2P too)
  - Valid Dictionary (**V**): Valid dictionary words not matching any other keyword
  - Mis-spelled (**Z**): Misspelled words

© 2019 Mobileum, Inc. All rights reserved. Confidential and Proprietary Information of Mobileum, Inc.

# Keyword Conversion

- SPAM
  - MSG: “your mobile no is selected as winner of 1000000 on sony sweeptake. go to www.dosony.net to claim. enter ref: son083ac . helpline: info.sony”
  - Keyword String: “VVSNCSDUSVZNZZZ”
- A2P
  - MSG: “Thanks for joining Westpac. Your SMS verification code to open your account is 34350. The code will expire in 10 minutes”
  - Keyword String: “DVZDOODSNOVNV”
- HAM
  - MSG: “Hope there are no more breakdowns! I can do city beach but won’t be there until about 12.30. I’ll see if Lynne can meet me at the clinic”
  - Keyword String: “DZVVZNZDZDV”

© 2019 Mobileum, Inc. All rights reserved. Confidential and Proprietary Information of Mobileum, Inc.

# Machine Learning

- Combination of unsupervised and supervised learning
- Target set reduced by looking at outlier messages using unsupervised learning
  - LSTM Auto Encoder (AE) used to learn patterns based on sequence of keywords
  - AE will learn the most common message which are HAM messages
  - Outliers will be A2P, SPAM and (few unique) HAM messages
- Classifier (supervised) used to remove HAM messages and differentiate between A2P & SPAM
- Feedback via case management used for improving accuracy and coverage
  - Classifier training
  - Auto encoder tuning
  - Classifier training
- User can provide feedback on keywords
  - New spam word or A2P specific word
  - Does not require training and ML approach uses keyword rather than actual words

© 2019 Mobileum, Inc. All rights reserved. Confidential and Proprietary Information of Mobileum, Inc.