infobip

Fraud challenges in the messaging ecosystem

Artificial SMS traffic inflation fraud

The unstoppable trend of using mobile devices for all aspects of daily lives, from communication to financial services and shopping has brought numerous benefits and convenience to users worldwide, in a way replacing the role of PCs. However, that shift to mobile devices has been also linked with an increase in mobile-based fraud, with numerous scenarios targeting users' financials, personal information and more. The most common threats are SMS phishing (also known as smishing), SIM jacking, and malware attacks through rogue apps or link. While they are different in the way they function, what they have in common is the goal to gather the user's personal and financial information or build up mobile charges by unwittingly subscribing to premium services. In all these cases, the damage is not only to the user, but also enterprises and mobile operators and their reputations.

With their SMS processing features, SMS firewalls can help identify not only well-known security threats and fraudulent traffic, but also new, previously unrecognized occurrences.

Latest type of messaging fraud detected

As the messaging ecosystem keeps growing, SMS as a channel is being misused for various fraudulent cases, with SIM farm-based A2P grey routes as one of the most frequent examples.

Thanks to existing fraud prevention toolsets sGate was able to detect **a peculiar SMS message content pattern that did not appear to be either A2P traffic, or legitimate P2P messaging**. The initial assumption, based on the random nature of the message text identified through a deeper analysis of message content, was that it was yet another cunning attempt by SIM farm operators to mask traffic and bypass A2P SMS charging rates.

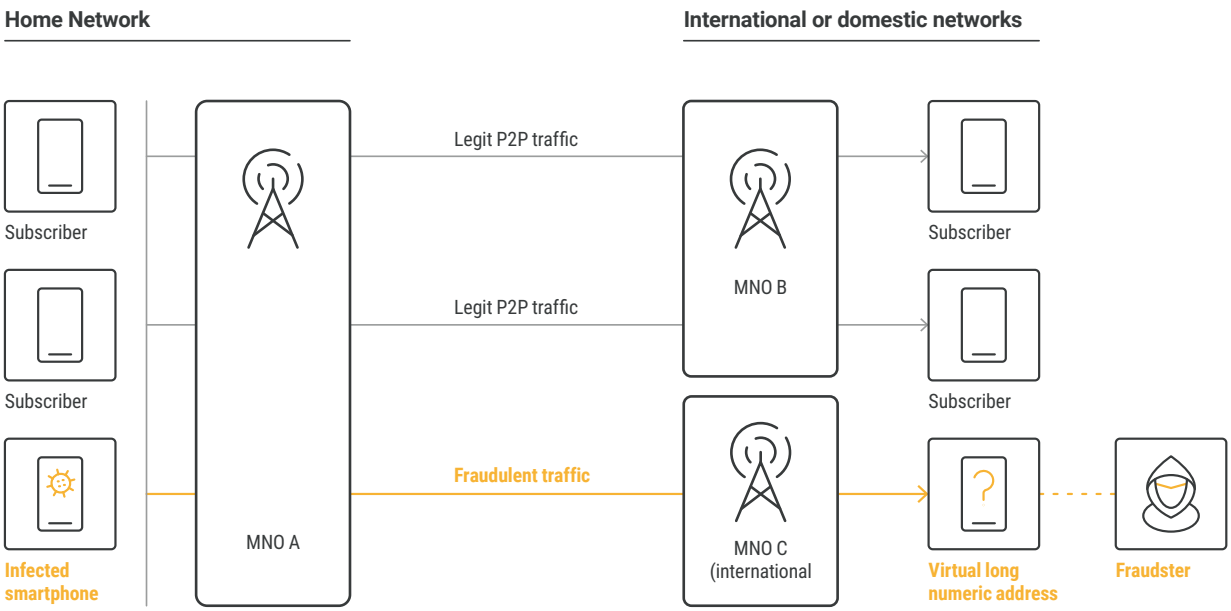
download games 508503942731765	***evaluations ruling occur tracked confusion 5001851718479380***	***your verification code is: 56437***
Spam-like example	**Random phrases**	**A2P SMS OTP-like**

The next assumption was that this was spam traffic, but after further analysis and coordination with the mobile operator, it turned out that senders were genuine subscribers and that **these messages were sent by subscribers, or more precisely, by their smartphone**. A telltale sign that this is potential fraud was the fact that message recipients were MSIDSNs in **international destinations with high message cost**. This meant that subscribers were incurring high charges and similarly, high roaming charges were accumulating for the operator.

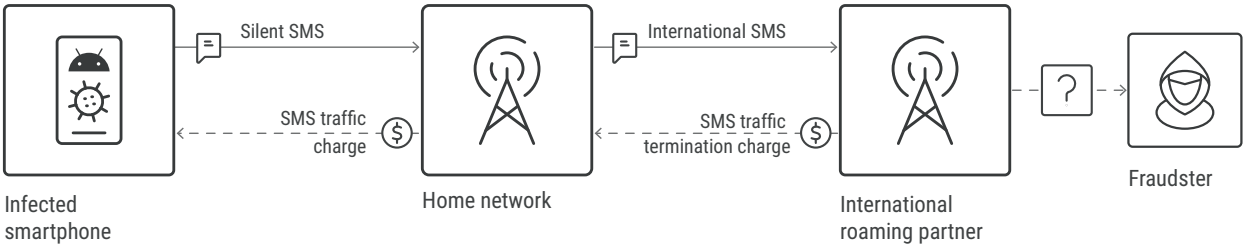
This is what the GSMA calls **Artificial Traffic Inflation Fraud,**, and it is driven by mobile subscribers sending international SMS messages over a specific app.

This can be a **conscious install of a fraudulent app**, but where the subscriber is not aware it is a fraud technique.

Another possibility is that an **app sends SMS messages without the user knowing**. This app can be an app posing as a legitimate, e.g. gaming app, or a fraudulent imitation of a legitimate app.



Through further analysis, this type of fraud was detected in multiple Infobip SMS firewall deployments, in various regions worldwide, suggesting that this was a global threat. Additionally, what little information is available about this fraud says that there were no reported cases on iOS devices. Android devices have more possibilities for users to sidestep built-in store safeguards and install unapproved and potentially unsafe apps which can spread malware or, like in this case, defraud both the user and the mobile operator.



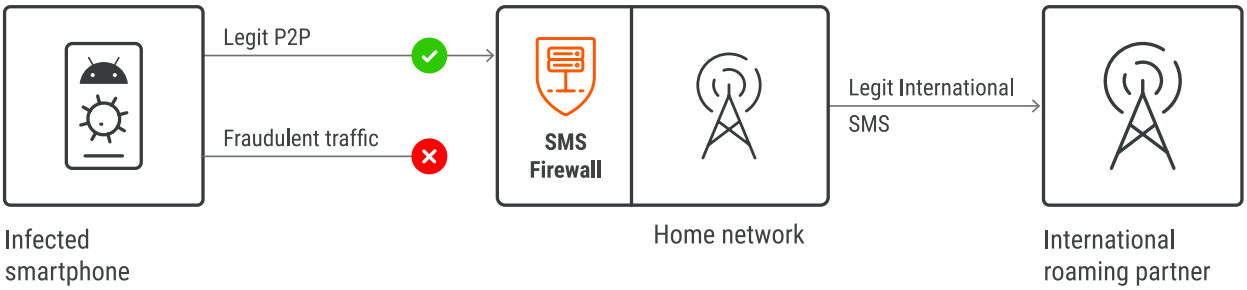
What currently remains unknown is just how fraudsters profit from this scheme, but destination mobile operators were notified of the issue and detailed fact- finding is still underway.

What next?

We've been able to conduct a wide-reaching investigation in multiple regions across the globe based on data available from Infobip sGate, which allowed us to alert mobile operators about this type of fraud.

For mobile operators, it is possible to dispute the fraudulently increased roaming charges, but that is a long process that does not guarantee both parties will reach an agreement. Detecting and preventing this type of fraud is currently the best way to protect the interests of MNOs as well as their subscribers.

Discovering this particular case of fraud has been a unique opportunity to work together with operator partners and further investigate to determine all the details of the fraud. We were also able to engage with sGate SMS firewall partners which were the among the first where the fraud was detected, and start **developing a solution to this issue**.



Features of this solution:

- Algorithm added to sGate to detect this particular fraudulent behavior and its elements:
  - International P2P SMS traffic – sent to distant and unusual destinations
  - Dynamic recipient range – similar or identical SMS traffic sent to multiple destination numbers
  - Abnormal traffic volumes – significantly differing from usual P2P SMS usage
  - No return SMS from international destinations – indicates no actual communication
- Automated decision-making by sGate SMS firewall to identify affected senders
- Traffic from such senders is automatically blocked by a single dynamic firewall rule simplifying the process and removing the tedious process of manually defining blocking rules based on sender and/or destination
- Traffic filtering can be fine-tuned to still allow domestic SMS traffic from affected users
- The list of affected subscribers is shared with the mobile operator, and then their customer care teams reach out to subscribers with tips on how to solve the problem
- Once the malware is removed from the smartphone of affected subscribers, the blocking rule is simply disengaged for solved cases or automatically deactivated after a specified period of time

This process has proven to be not just efficient in rapidly putting a stop to fraudulent traffic, it is also extremely accurate, yielding **less than 0.1% of false-positive cases**.

Conclusion

This new fraud case is only further proof that the SMS ecosystem is evolving and with it the potential for fraud. The fact that it was discovered by an SMS firewall shows that SMS firewalls have a use beyond detecting and preventing SMS charging bypass, and that they are effective and flexible enough to adapt to evolving fraud scenarios. **The focus of fraudsters in the dynamic SMS ecosystem renders proper network protection not an option, but a necessity for every mobile operator**. While it is difficult to identify all possible sources of fraud because they are always discovered retroactively, operators are not defenseless. They are still able to efficiently mitigate the problem by blocking fraudulent traffic while the issue is being addressed between operators and technology partners.

Moving forward, industry players need to engage and work closely together in identifying and fighting emerging fraud cases. It does require a wider action by the mobile ecosystem, but it is the only proper way to guarantee transparency and security, and a mobile ecosystem where everyone prospers – mobile operators, technology vendors and, ultimately and most importantly, mobile users.

The Infobip Advantage

GLOBAL REACH AND LOCAL PRESENCE

- 600+ direct-to-carrier connections
- Connect with over 7 billion people and things
- Strong enterprise client base
- 60+ offices on 6 continents

Our local presence enables us to react faster and have everyday interactions with our customers, providing solutions in-line with their needs, local requirements and based on proven global best-practices.

SCALABLE, FAST AND FLEXIBLE SOLUTIONS

- Best-in-class delivery rates
- High speed and reliability
- Low latency
- In-house developed platform

Our solutions are created to adapt to the constantly changing market and communication trends at speeds and levels of precision and personalization that only an in-house solution can offer.

REMARKABLE CUSTOMER EXPERIENCE

- Technical expertise
- Solutions consultancy
- Customer success management
- 24/7 support and network monitoring

Our solutions are created to adapt to the constantly changing market and communication trends at speeds and levels of precision and personalization that only an in-house solution can offer. We will help you to get up and running in no time, whether it's assisting with integrations, messaging best

OWN INFRASTRUCTURE

- Locally available services
- Compliance to local regulations
- 28 data centers worldwide

Our worldwide infrastructure easily scales horizontally, leveraging the hybrid cloud model to never run out of resources. Our built-in global compliance engine is constantly updated with the latest in-country regulations and operator requirements.

Best Customer Engagement Platform 2020

Best Global SMS Service Provider - Wholesale Solution 2020

ROCCO

Best A2P SMS vendor as rated by MNO's 2017, 2018, 2019 & 2020

Best A2P SMS vendor as rated by enterprises 2019 & 2020

Tier 1 SMS firewall vendor 2017, 2018, 2020

Top 10 inovator of 2020

Future Digital Awards

Recognising Challengers and Disruptors

JUNIPER RESEARCH

Platinum award as the Global CPaaS provider in 2020

Platinum award as the EMEA CPaaS provider in the 2020

Platinum award as the Best RCS provider in 2020

Gold award as the best Digital Identity Solution in 2020

MESSAGING & SMS GLOBAL AWARDS 2019

Best OTT Partnership 2019

Best messaging innovation - best RCS implementation 2019

4X AWARD WINNER

Best messaging API

Best messaging innovation-carrier solution

Best anti - fraud innovation

Best SMS / A2P provider for the EMEA region

mobile connect

PCI DSS COMPLIANT LEVEL 1 SERVICE PROVIDER

ISO 9001 ISO 27001 BUREAU VERITAS Certificatio

www.infobip.com