SecurityGen
Telecom Security. Transcending Generations.

SIGNALLING THREATS IN LATAM

LATAM Scenario

The insights shared in this document are drawn from the actual data collected by SecurityGen team across many MNOs (Mobile Network Operators) in the region.

Hard Truths

The number of attacks does NOT depend on the size of the country/Mobile Operator.

The volume of attacks received by an MNO depends on how vulnerable is the operator's signaling infrastructure and the efficiency of its protective systems, when available.

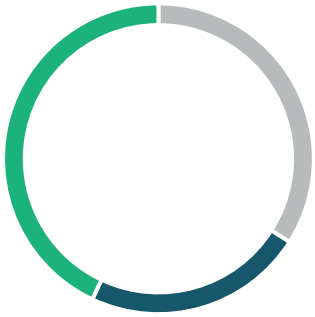
Attackers will always take the easier path. Unless there is a special contract with specific targets, they will focus on opportunities for a fast cashflow.

Some Numbers

- Operators received from **60 to over 100** thousand attacks daily.
- MNOs without a well configured firewall protection or not even STP and DEA protection, had an average of **70% of incoming attacks** being successfully responded by the network. Due to nature of some attacks (like sweeping), this is expected.
- When protective measures are executed on the network correctly, successful attacks drop to **less than 1%.**

Attack Categories

The most common exploited threats were:



- Fraud
- Data Breach
- Subscriber DoS

Considerations

- The largest category - Fraud - mostly comprises of such attacks against MNOs as grey route and SMS and Billing evasion.
- Data breach mainly was against subscribers and included IMSI, location data and interception of calls and SMS. In many of those events, cross-protocol attacks were performed either to facilitate or obfuscate the main attack.
- A minor part in terms of volume, the Operator data breach is still much relevant if you consider the possibility of network mapping and posterior Denial-of-service.

- Subscriber DoS is not evenly spread worldwide but is unfortunately detected in some countries in the region. If you assume part of the subscribers is IoT equipment used in utilities and security, DoS attacks are considered significant threats to the general public.

Want a better understanding of how those threats affect your Operator and how to Identify, Detect and Protect the Network and Subscribers?

Just reach out for a clarification session at contact@secgen.com, and we at SecurityGen will be happy to guide you through a completely new approach to securing your Network and Subscribers!