:: Positive Technologies

SIGNALING THREATS IN THE WILD

Characteristics of Attacks

DISTRIBUTED IN ORIGIN

Part of subscribers have received attacks from different carriers, and it is perceived that a reduction in sending by one source is sometimes reflected in an increase in another.

CONCENTRATED IN DESTINATION

Less than 1% of subscribers usually receive most of the attacks. Exception for IMSI sweeping campaigns.

NOT REPUDIATED

80% of victims received more than one attack

44% of victims received more than one type of attack.

5% received 4 or more types of attack

HAPPEN IN WAVES OR ESSAYS FOR LATER EXPLOIT

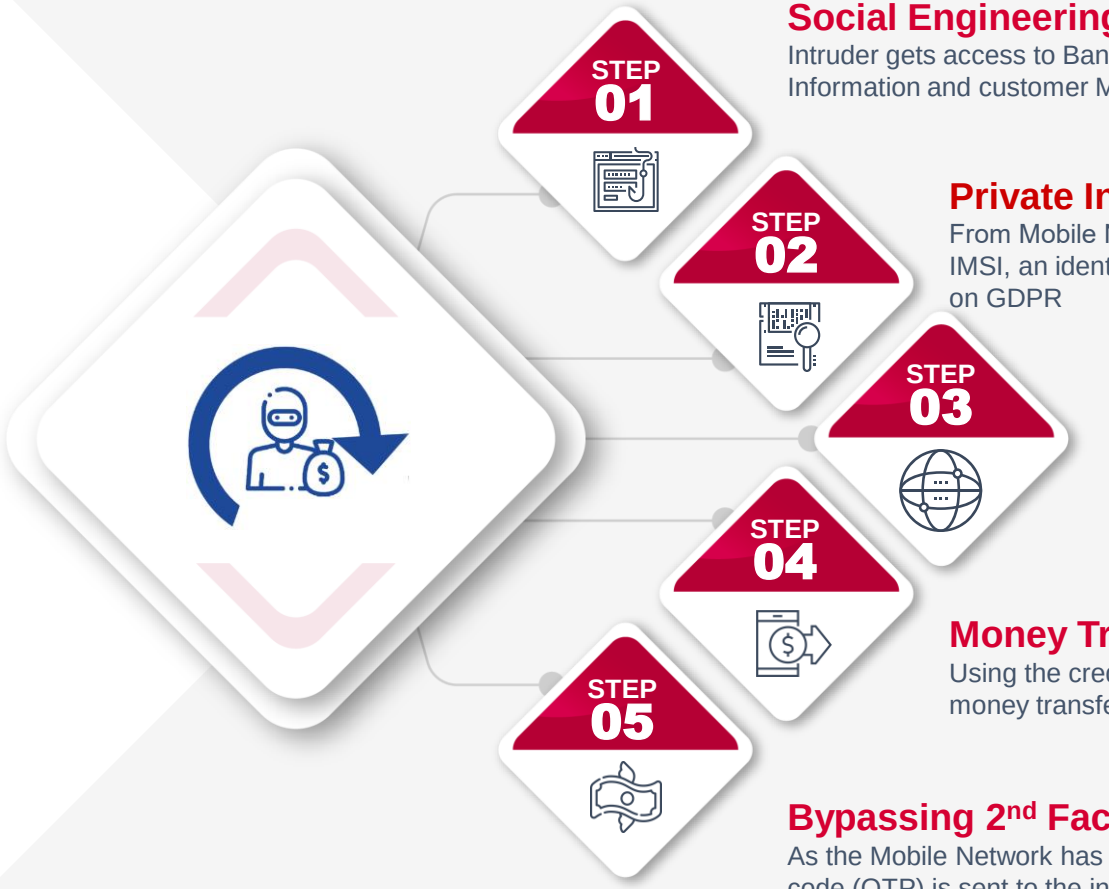
After months of monitoring with low incidence of USSD attacks, we identified an intense and non-repudiable action, for example.

That shows the relevance of Assessments in accelerating protective actions.

Banking Fraud Operation

This is the portrait of an **ongoing** online banking fraud campaign **Positive Technologies** has identified in some countries.

MNOs may prevent this fraud by protecting their networks from the threats described on steps 2 and 3.



Social Engineering (Likely)

Intruder gets access to Bank Account Information and customer Mobile Number

Private Information Leak

From Mobile Number, intruder discloses customer's IMSI, an identifier which is considered Personal Data on GDPR

Tampering with the Network

A fake registration is made for the subscriber, changing its location to a fake one

Money Transfer

Using the credentials from **Step 1**, intruder order a money transfer from subscriber bank account

Bypassing 2nd Factor Authentication

As the Mobile Network has accepted a fake location **(Step 3)**, the SMS with code (OTP) is sent to the intruder and transfer is successful.

How to avoid it?

Start taking protective actions at once, in order to mitigate:

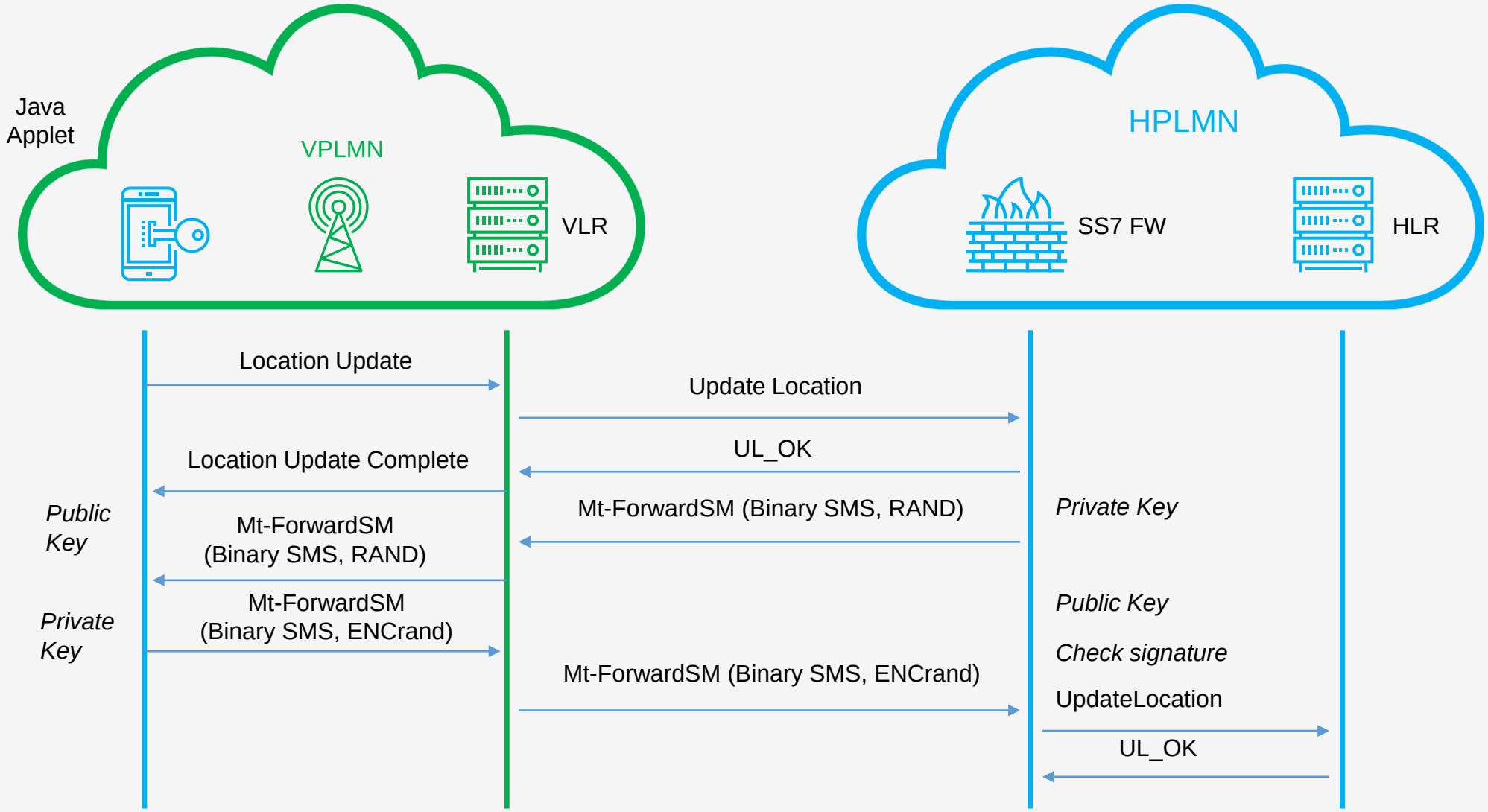
- **The Fraud Itself**
- **Privacy laws sanctions due to data leaks**
- **Impacts on Service Availability**

Take action to continuously **Monitor and Block attacks.** Usual techniques include:

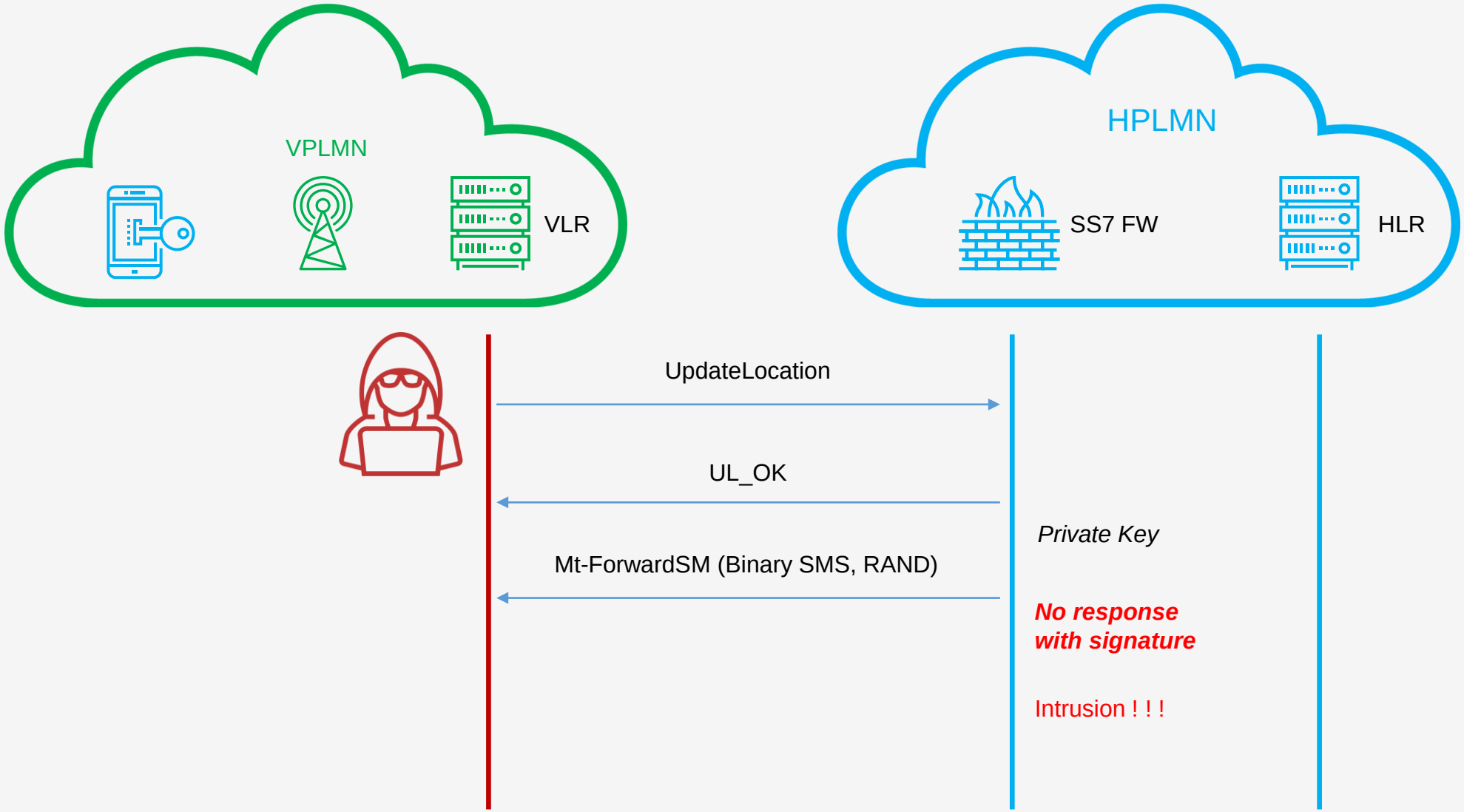
- **Velocity Check**
- **Active Network Interrogation**

But what else could be done?

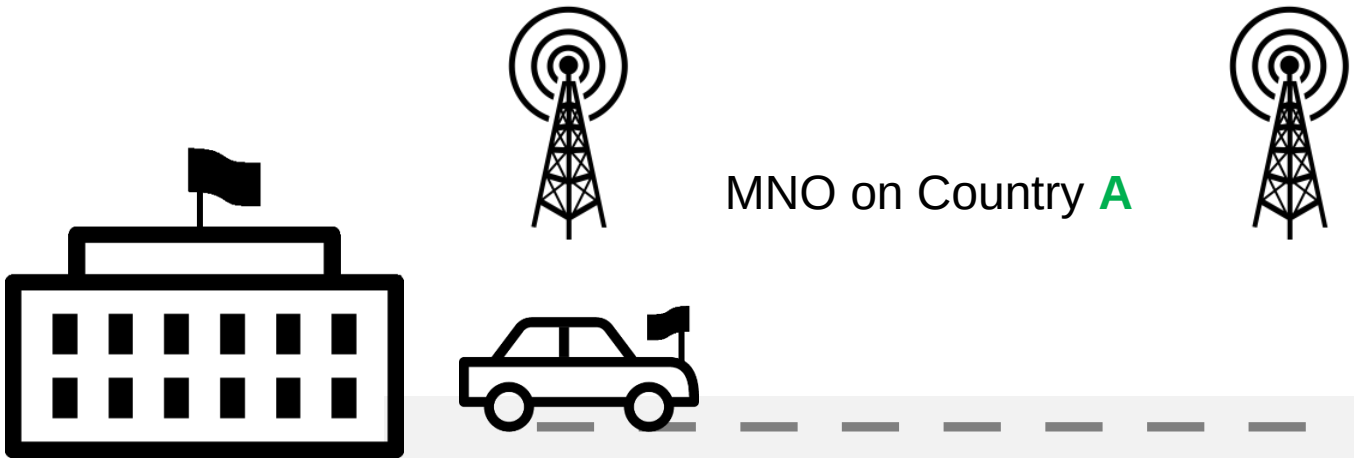
Authenticating Subscriber Location



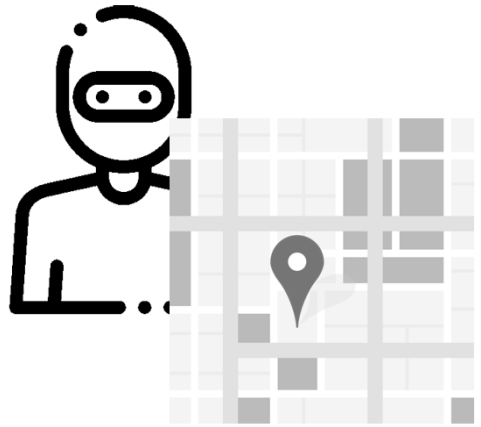
Authenticating Subscriber Location



International Affairs



Consulate
from country **B**



Consulate’s employee location being collected every 3 minutes at country **C** through **SS7 signaling**

It may look like a Hollywood movie but is a real (and non repudiable) attack discovered at one of our customers. The MNO has taken action to stop the collection right after learning about it.

Multinational attack

- **Phase 1:** Two messages from Country 01 collect IMSI and Location from a Subscriber in Country 02
- **Phase 2:** One message from Country 03 improves the location accuracy from the same Subscriber
- **Phase 3:** A final message from Country 01 collects the location information once again

:: Positive Technologies

Thank You