SMS Phishing & Malware Spreading attacks

Know the difference

openmindnetworks.com

Smishing Verus Malaware

SM S Fraud has been widely documented and discussed, but many people remain unaware of the clear distinction between the two distinct types of attacks that Fraudsters are employing. B oth attacks need to be stopped, but that can only be done if the solutions and counter-measures Operators put in place have the necessary functionality to detect and block the two different attacks.

The two attacks that need to be stopped are 1. SM S Phishing (Smishing) and 2. Malware Spread by SM S (e.g. FluB ot). B oth attacks have different characteristics and have distinct goals that cause damage to mobile operator networks and subscribers in a number of different ways.

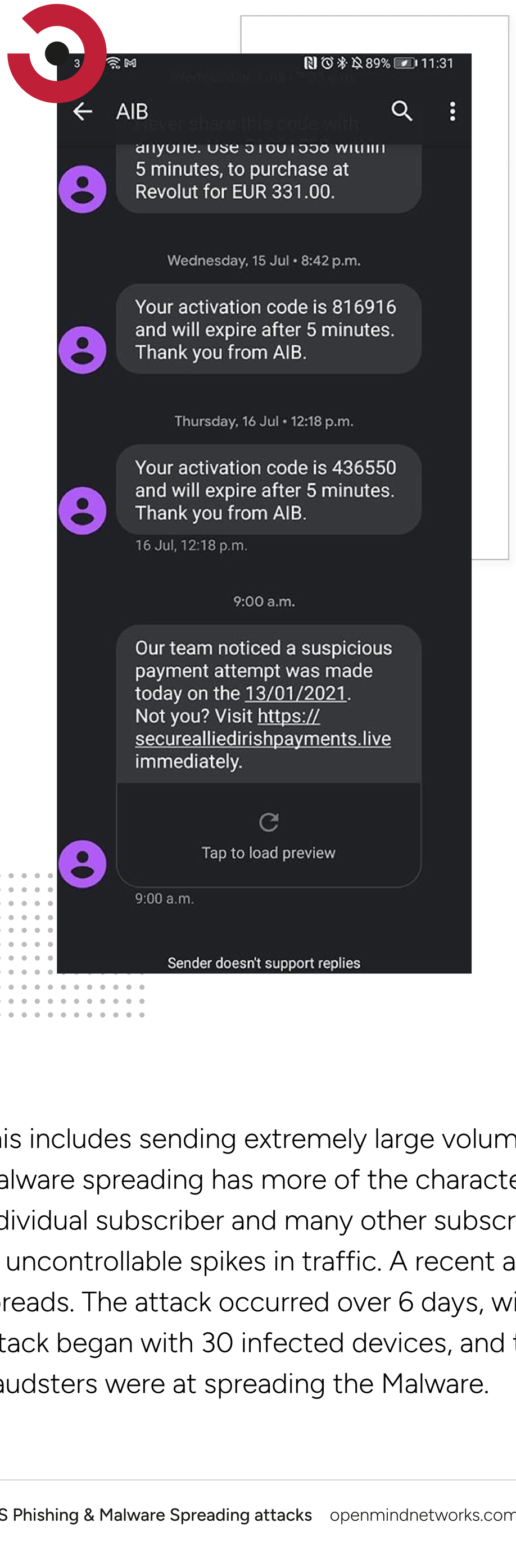
Smishing

Smishing messages contain fraudulent URLs with the goal of luring subscribers into revealing Personal or Account access information. Typically, the messages appear to be from a Bank, C redit Card C ompany, or from a high value Service Provider such as Apple. The most dangerous situation is when the same Origination Address in a Fraudulent message is also used for legitimate messages. W hen this happens, the fraudulent messages appear in the same ‘thread’ as real messages, and subscribers are more likely to fall victim to the fraud.

Smishing messages can be sent via Aggregators or from Mobile devices. The volume of actual Smishing messages sent in any one campaign can be relatively low, as the Fraudsters may be paying aggregators to deliver messages on their behalf. This requirement to fund the fraud puts a restriction on the number of messages.

Many operators and banks have focussed their efforts on educating subscribers and customers about the risks associated with receiving unexpected messages. There have been various attempts in different countries to enforce measures to reserve the use of specific Origination Addresses for validated senders.

Two Different Forms of Smishing Messages



From a Mobile Number

This Text is Legitmate Origination Address is Spoofed as a Bank name (AIB).

This Text is Fraudlent In order to detect and stop Smishing attacks, solutions used by O perators need to be able to identify ‘spoofed’ messages apparently from Banks but containing modified URLs. Solutions need to be sensitive to quite low volumes, and be tuned to recognize ‘banking’ messages from unauthorized sources. Smishing tends to happen at a relatively stable level over a long period of time. The fact that fraudsters need to keep the message text authentic-looking can be used by monitoring software as a means to identify the fraud.

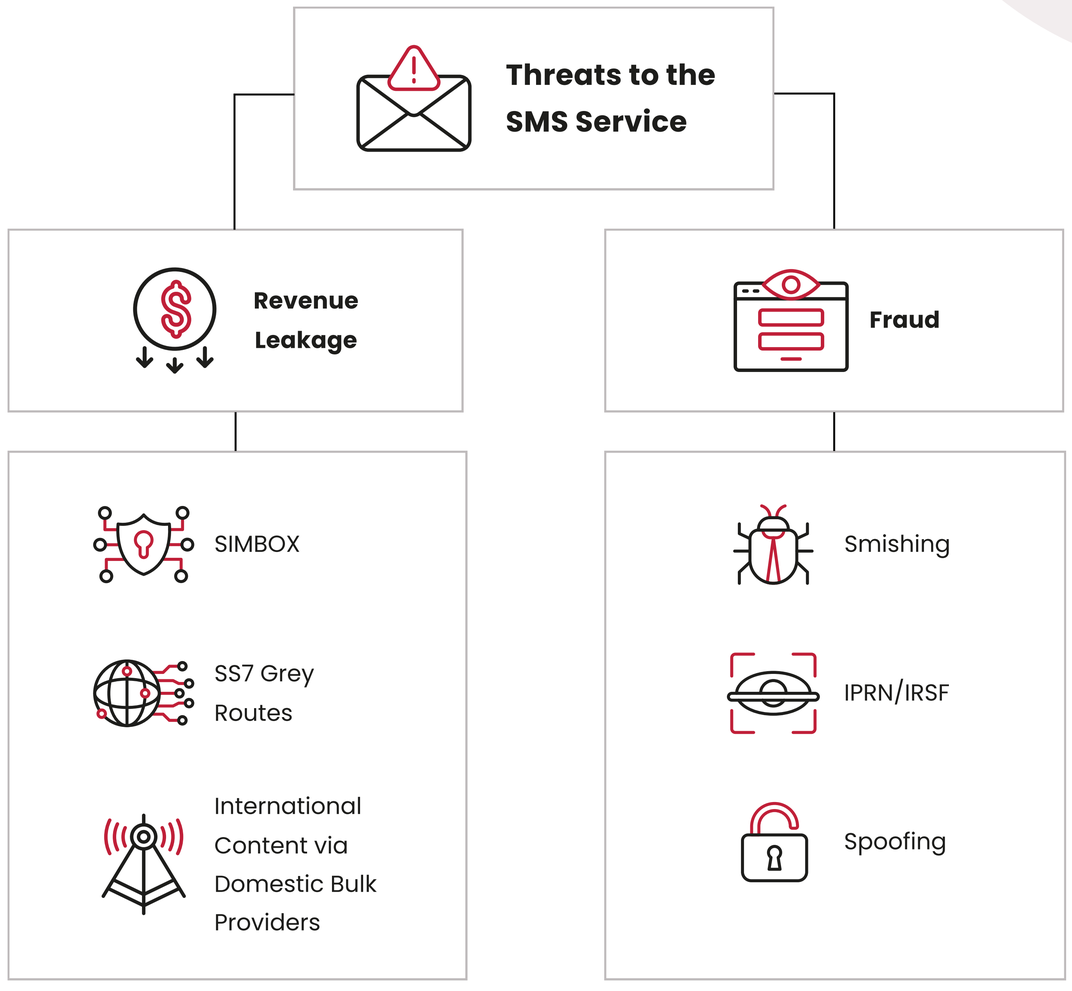
Malware Spread Attacks (FluBot)

The goal of attacks like FluBot is to try and convince as many subscribers as possible to install Malware on their phones. Once Malware is installed on a phone, it becomes part of a Botnet - a network of hijacked devices remotely controlled by Fraudsters. While FluBot itself is typically described as a Banking Trojan that aims to obtain bank access details by monitoring Bank App usage, a hijacked device can be **exploited by** Fraudsters for multiple purposes.

This includes sending extremely large volumes of text messages to the next victims of the fraud. Malware spreading has more of the characteristics of a cyberattack that can cause financial loss to an individual subscriber and many other subscribers, while also potentially damaging the network itself due to uncontrollable spikes in traffic. A recent attack Openmind observed illustrates how the Malware spreads. The attack occurred over 6 days, with messages being sent in bursts at regular intervals. The attack began with 30 infected devices, and the growth rate of active Bots shows how successful the fraudsters were at spreading the Malware.

This is why FluBot and similar attacks have come to the attention of National Security and Defence officials in many countries around the world. Relatively small numbers of infected devices on a Botnet can initiate a Denial-of-service attack, and by overloading signalling channels can effectively take down a network.

FluBot is a cybersecurity threat, and not just a means of defrauding unwary subscribers. FluB ot is both cruder and more insidious than a typical Smishing attack. Because the Fraudsters have free access to messaging via the devices they control on the BotNet, they are unlimited in the number of messages they can send. This results in waves of FluB ot that can generate millions of messages targeting a network in a short period of time. FluB ot attacks are typically recognised therefore by sharp spikes in load on the network, and by massive increases in interconnect costs.



Compared to Smishing messages however, individual FluBot messages can be harder to recognise. While Smishing messages need to closely match banking messages to be successful, FluBot messages can appear to be from anywhere, as the aim of the Fraud is to have malware installed on the phone that can subsequently be used to capture bank details. This type of in-direct attack is harder to recognise.

”

As FluBot attacks use a potentially unlimited variety of texts and URLs, the focus of FluB ot prevention needs to be on detecting unblocking the sending devices.

About Openmind Networks

Openmind are world leaders in mobile messaging. Our consolidated and flexible platform, delivered via a DevOps process, provides our Mobile Operator, Wholesale Operator and Messaging Aggregator customers with new revenue-driving opportunities at the lowest total cost of ownership.

Get in touch with us now:

+ 353 1 633 0070

+ 353 1 670 8008

sales@openmindnetworks.com

Twitter Linkedin Youtube

Deloitte.

IRELAND BEST MANAGED COMPANIES

GOLD STANDARD WINNER

Winner of Deloitte Best Managed Company Five Years Running 2015 - 2019

openmind
WE ARE MESSAGING

Delivering and Connecting more Messages between International Mobile Operators than any other Vendor in the World

Silicon Valley | Dublin | Amsterdam | Prague | Dubai | Kuala Lumpur