ENEA
AdaptiveMobile Security

CASE STUDY

Messaging Security in Latin America

A leading Tier-1 mobile operator in Latin America selected AdaptiveMobile Security to resolve the problem of SMS messaging abuse that was causing major service issues for their subscribers.

Their network was previously unprotected from SMS messaging abuse and threats, and investigations had shown that large amounts of spam, including messages phishing for subscribers' personal financial information were present in considerable volumes.

By implementing the AdaptiveMobile Network Protection Platform (NPP) in conjunction with AdaptiveMobile's Threat Intelligent Unit (TIU) Messaging Security service, the operator was able to address these issues, initially allowing them to identify and then subsequently disconnect large numbers of problem spammers from their network and block new messaging abuse as it emerged.

Overview

Situation:	Mobile operator in Latin America experiencing major challenges with marketing spam and financial phishing SMS messages.
Solution:	AdaptiveMobile's Network Protection Platform (NPP) supported by AdaptiveMobile's TIU Silver Messaging Security Service.
Success:	Accurate identification and eradication of SMS spam and phishing traffic from operator's network. Ongoing disconnection of persistent spammers and blocking of new messaging abuse.
Impact:	Future protection for mobile subscribers and increased trust in the operator's mobile messaging brand across the LatAm region.

The Situation

A tier-1 Mobile Network in Latin America had been experiencing a growth in the number of subscriber complaints relating to Spam and Phishing messages present on their network.

Messaging abuse or spam are messages that are sent by various groups, ranging from and including:

- Simple over-aggressive marketing companies whose recipients have not signed up
- Payday loan merchants trying to push aggressive loan products
- Phishers who are trying to obtain financial credentials and login details for websites
- Bank account attackers trying to fool user into ringing up automated helplines in order to gain access to their accounts

A range of nefarious spam and phishing messages have been found on this particular network, the most predominant being bank and credit card phishing messages. Actual examples seen include:

ALERTAS BBVA BANCOMER: Su tarjeta BBVA BANCOMER ha sido bloqueada por seguridad, ingresa en el siguiente enlace para activarla https://XXXXXXXX

English translation:

Your XXXXXXXX card has been blocked for security, enter the following link to activate it https://XXXXXXXX

Su Apple ID fue usado para iniciar sesion en iCloud mediante un IPhone (https://apple.XXXXXXX)y verifiquesusdatos.ï£¿AppleInc

English translation:

Your Apple ID was used to log in to iCloud through an IPhone (https://apple.XXXXXXX) and verify your data. ï £ Apple Inc

However, a range of other spam messages also appear, with common examples such as.

Soy DR Tobi, llamo pero su telÃ©fono no puede ser alcanzado, me entra en contacto con aqui(XXXX@gmail.com) para el negocio que beneficiara a ambos nosotro

English translation:

I'm DR XXXX, I call but your phone can not be reached, contact me here (XXXX@gmail.com) for the business that will benefit both of us

Aware that the impact of not addressing such threats on their network would result in bad publicity for themselves and other operators within their group, and ultimately subscriber churn, they turned to AdaptiveMobile Security to address this difficult issue and turn their messaging service into a high quality and trusted experience for subscribers.

Choice of AdaptiveMobile

The AdaptiveMobile Network Protection Platform (NPP) in conjunction with the TIU Messaging Security Service was the ideal choice to resolve the challenges the operator faced.

The operator understood that AdaptiveMobile would very rapidly be able to bring a wealth of knowledge with real-world experience gained in over 50 messaging security deployments globally.

Solution

The Network Protection Platform (NPP) is a converged carrier security platform proven on global scale in the most demanding of carrier environments, from high performance networks in North America, to massive scale networks in India, to the unique challenges of African networks.

Key technical considerations that made the NPP the ideal choice for the customer's situation included the following:

- The NPP is designed for carrier grade scale and performance. It is proven in some of the largest messaging environments in the world.
- It's real-time system-wide reputation capabilities are ideal for accurately and confidently identifying spammers. It allows targeted inspection of suspect sources, providing a constantly updated view based on prior behaviour, with sophisticated aging techniques that also incorporates positive source behaviour (see figure 1).
- It's Industry-leading tamper-resistant spam and phishing fingerprint techniques ensures spammers are not able to metamorphosise their Spam messages and bypass active blocking filters.
- It's sophisticated new threat discovery with proprietary algorithms constantly hunt for and identify suspicious new threats, delivering up to zero-minute protection (see figures 2 and 3).
- The NPP also features Industry leading false positive accuracy for messaging security achieving a false positive rate of 2.1 messages per 1 billion messages processed.

In addition, the TIU, through their Silver Messaging Security Service, and utilising experience from their leading mobile security experts, provides active review of the customer's network traffic, enabling creation of new configurations to tackle the latest and emerging threats.

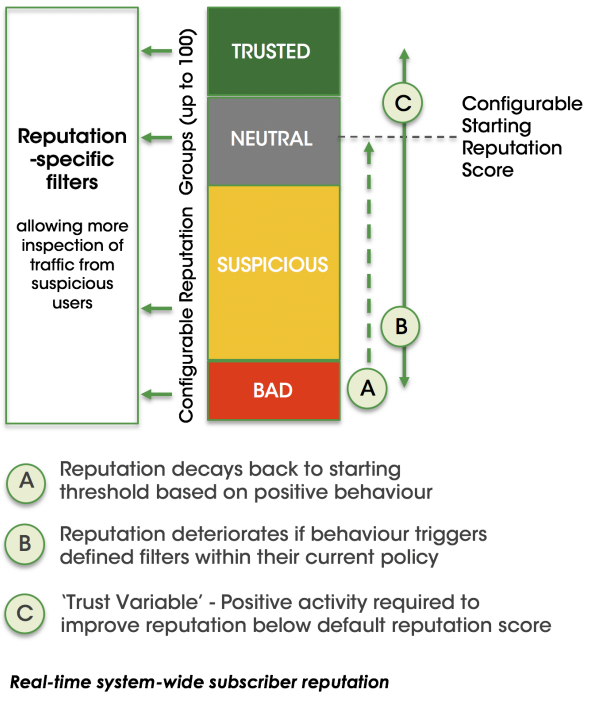

Figure 1: Real-time system-wide subscriber reputation

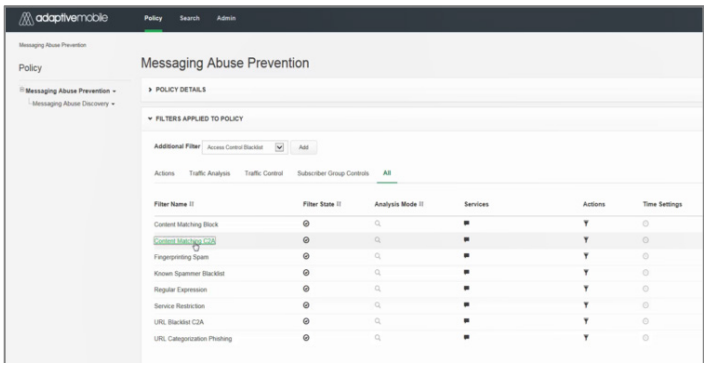

Figure 2: Policy Management: Sophisticated new threat discovery

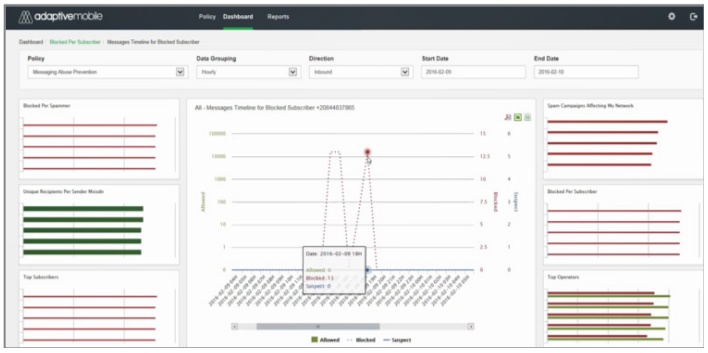

Figure 3: Comprehensive Reporting: Drill-down to threat details

Results

In 2016, shortly after initiation of the TIU Silver Messaging Security Service, and after a short period of analysis and fine tuning, spammers were rapidly driven off the network and the number of subscribers that required suspension decreased rapidly.

Figure 4: Spammers and Phishers initially driven of the network

Outcome: Complete Protection for the Subscriber

In the last year, with around 2 to 5 billion messages processed by the NPP per month, the blocking rate has remained relatively consistent. The initial high volumes of spammers and phishers have been dealt with in 2016 and ongoing, new spammers and phishers are not able to penetrate the operator's new defences. Note, it's not always about stopping abuse entirely, but creating a hostile environment for attackers who must then move on to easier unprotected targets as their ROI disappears.

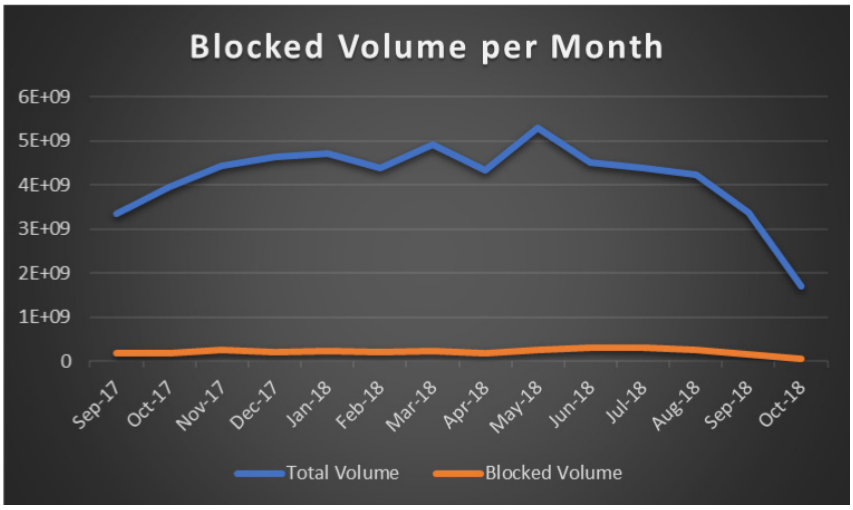

Figure 5: NPP scaling to protect network with billions of messages per month

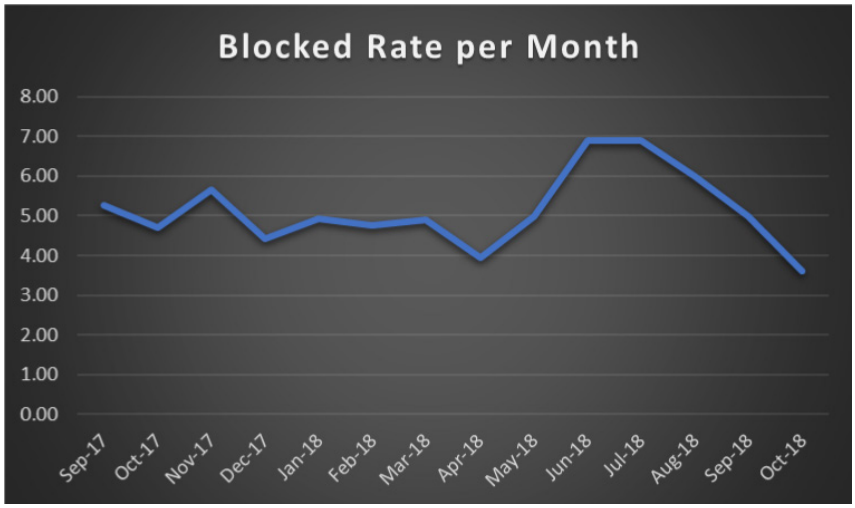

Figure 6: Ongoing blocking rate levels following initial irradiation of problem spammers and phishers

AdaptiveMobile Security has earned the trust of the operator for its ability to handle a range of messaging challenges, both current and future. This has helped to deepen the relationship with the operator. The success has also opened up expansion opportunities in LatAm across other properties in the operator's group.

All in all, the operator is very pleased with the dedication and sense of partnership that AdaptiveMobile Security have brought to the table to complement their technical expertise. They know that, thanks to AdaptiveMobile's unique and proven solution, a system has been put in place to address ongoing and future messaging threats, thus protecting its most important asset - its subscribers.

About Enea AdaptiveMobile Security

Enea AdaptiveMobile Security is a world leader in mobile network security, everyday protecting over 80 Mobile Operators and billions of mobile subscribers and devices globally from fraudsters, criminals and nation states. We have the strongest 5G core network security team, who are designing, planning and building the very best in 5G core network security solutions focussing on threat-intelligence, security heritage and protocol correlation.

Enea AdaptiveMobile Security brings a unique security perspective on real-time mobile network traffic. The global insight provided by our 5G, Signalling and Messaging thought leaders, security specialist teams and Threat Intelligence Unit, combined with our signalling and network protection software that sits at the heart of the network, ensures Enea AdaptiveMobile Security remains at the forefront of the latest advancements in mobile networks and their security, and continues to be the trusted partner of many of the world's largest Mobile Operators.

For more information on how Enea AdaptiveMobile Security can help you protect your communications infrastructure, subscribers and revenues, please contact **sales@adaptivemobile.com**.

Legal Notices

HEAD OFFICE

Ferry House, 48-52 Lower Mount St, Dublin 2.

Contact: sales@adaptivemobile.com

www.adaptivemobile.com

REGIONAL SALES CONTACT NUMBERS

US, Canada, Latin America Sales: +1 972 377 0014

UK Sales: +44 207 049 0421

Middle East Sales: +97144 33 75 83

Africa Sales: +27 87 5502315

Asia Sales: +65 31 58 12 83

European Sales: +353 1 524 9000

REGIONAL OPERATIONAL SUPPORT CONTACT NUMBERS

UK: +44 208 584 0041

Ireland: +353 1 514 3945

India: 000-800-100-7129

US, Canada: +1 877 267 0444

LATAM: +525584211344