adaptivemobile™
trusted network protection

Network Protection in the Middle East

A Tier-1 operator in the Middle East – a member of one of the biggest Telecommunications Groups in the world – selected AdaptiveMobile to identify and resolve issues relating to messaging traffic that had been observed in the network. Investigations had shown that mobile devices were generating SMS and MMS traffic that was not visible to the subscriber and the operator was concerned over network impact and potential fraud against their subscribers. By implementing the AdaptiveMobile's Network Protection Platform (NPP), the operator was able to identify and resolve the issues.

Overview

- **Situation:** Mobile operator in the Middle East experiencing challenges with SMS and MMS traffic
- **Solution:** AdaptiveMobile's Network Protection Platform (NPP)
- **Success:** Identification and prevention of SMS & MMS malware traffic from network. Disinfection of infected subscribers
- **Impact:** Elimination of SMS and MMS malware. Future protection for subscribers.

Situation

A tier-1 Mobile Network in the Middle East with about 4 million subscribers had been experiencing a growth in the number of subscriber complaints relating to messaging. Subscriber bills reflected (SMS and MMS) messages that were sent from the handsets, but of which the subscribers denied all knowledge. The unexplained traffic was having a major unplanned impact upon the operator's SMS and MMS infrastructure causing loss of revenue; as well as adding to the operating costs of the operator, due to the increased traffic requiring an increase in SMSC and MMSC license and capacity.

Further examination of the traffic established a trend of messages being terminated to specific mobile numbers. It was also observed that the numbers that these messages being sent to were not valid subscriber numbers on the network.

Apart from the fact that there was a significant increase in the number of reported subscriber care events relating to these challenges, the operator was also witnessing subscriber churn. As part of measures to this churn, a plan was put in place to identify and address the service deficiencies that had contributed to an overall negative experience for their subscribers.

Choice of AdaptiveMobile

The AdaptiveMobile Network Protection Platform (NPP) was the ideal choice to resolve the challenges the operator faced, as it is able to address the specific way in which SMS and MMS spam is created. As shown in Figure 1, email spam filtering techniques are ineffective for addressing SMS. The 'text-only' mode of SMS; along with the local nature of TXT SPK (i.e. the language of SMS and MMS, which involves a lot of words being spelt in shorthand) complicate the task of monitoring messages for Malware.

The NPP also offered the operator a scalable solution, able to filter traffic across all bearers in real-time, taking into consideration the policies set by the operator, the permissions for sender and recipients, and the content of the SMS and MMS message being sent.

AdaptiveMobile's extensive experience in addressing cross-bearer threats was another reason for selection by the operator. AdaptiveMobile are currently filtering traffic for over 1 billion subscribers worldwide. This wide footprint meant that AdaptiveMobile could utilize their worldwide threat database on all bearers (not just SMS and MMS) and apply it within the network to handle current and future threats for the operator.

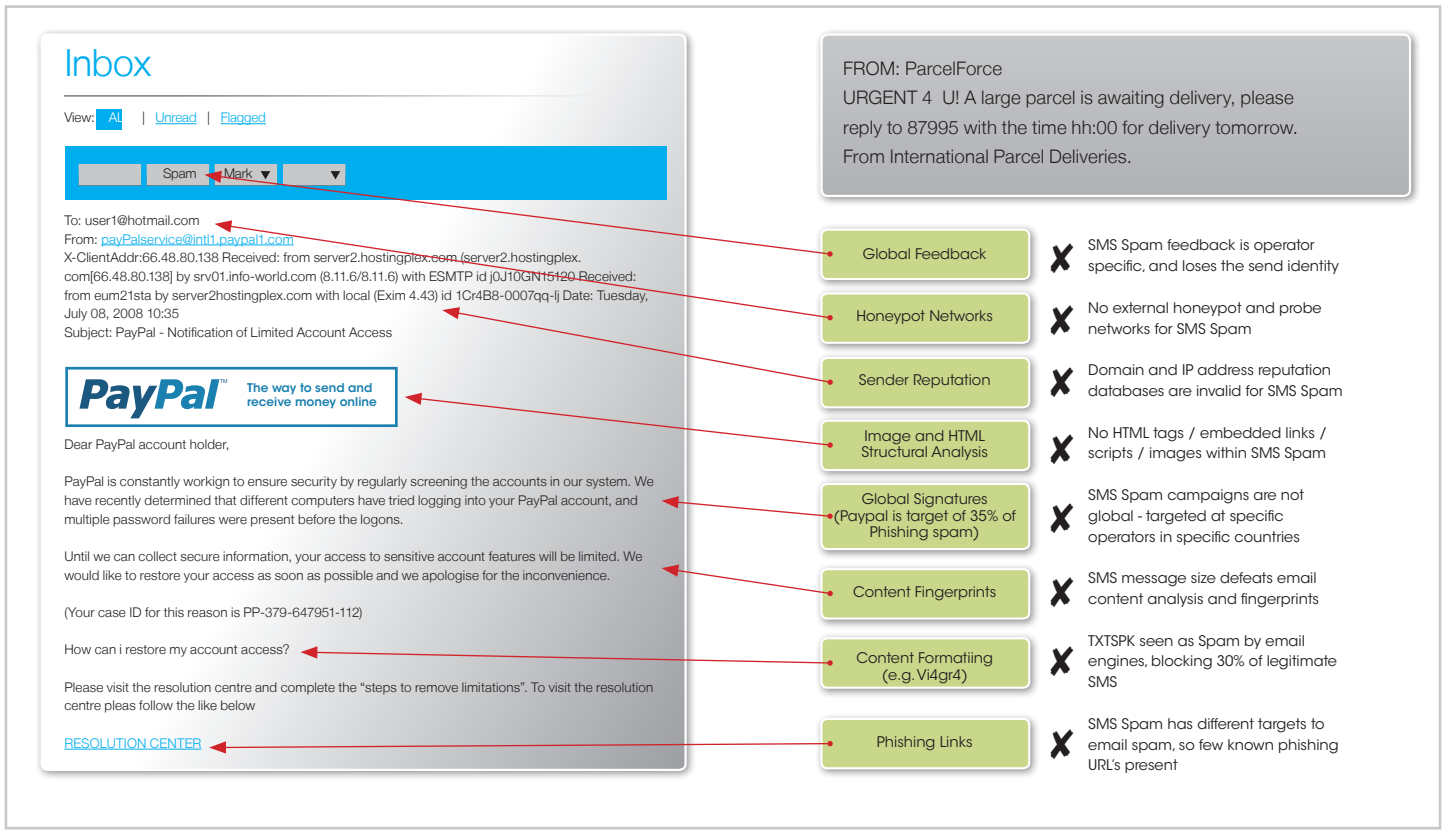

Figure 1: SMS Malware vs. Email Malware

Solution: Policy Filter and Malware Recovery

The operator deployed the Network Protection Platform (NPP) to filter SMS and MMS spam, malware and inappropriate content; in addition to implementing personal policy based blacklists, subscription controls and time-of-day controls. Also deployed was the AdaptiveMobile Malware Recovery Module (MRM), which works to notify infected subscribers of any Malware that reside on their devices and attempts to disinfect these handsets and laptops by distributing a disinfect cleaner. Together, the operator has a full solution to identify infection, protect the network from the symptoms, and then treat the root cause of the infection.

The NPP approach to resolving the challenges involved the following steps:

Monitor

- **Message volumes per sender:** subscriber SMS and MMS traffic was monitored for traffic anomalies, including sudden surges in traffic to and/or from specific subscribers.
- **User and traffic reputation and history:** subscribers were also monitored based on their history (e.g. with Spam).

Inspect

This involved monitoring for suspicious content (e.g. malware related Text, URLs) and traffic to and/or from blacklists, whitelists.

Control

- **Policy Controls:** Blacklists, Whitelists, Time-of-day restrictions are applied as per the setup configurations done by the subscriber or operator.
- **Block illegitimate traffic:** known spam, bots and virus traffic are blocked
- **Quarantine:** certain suspicious traffic and senders are quarantined for manual review and release (if necessary)
- **Alerts and Disinfection:** devices that have become infected with known Viruses and Malware are notified and disinfected as applicable.
- **Update user and traffic reputation**

Results: Detection and Elimination of Messaging Fraud and Virus

A summary of what was discovered, after the successful implementation of AdaptiveMobile's NPP within the network, is given below:

SMS: over 20% of the SMS traffic generated to or from subscribers on this network was either illegitimate or inappropriate. These can be classified into:

- Up to 12% of (inbound and outbound) messages that are terminated on the operator's SMSC were attributed to the Guardian Hati Hati virus[1]. These messages were blocked to prevent further effects for the infected subscriber and impact on the operator's infrastructure and costs.
- It was also identified that another 11% of SMS traffic showed signs of previously unidentified Malware. AdaptiveMobile's advanced signature filters were used to successfully identify and subsequently protect against this malware type, which was a unique new form of infection.
- SMS spoofing[2] was also identified. There were cases of spoofing traffic that was being received at the network, but ultimately targeted at operators in Western Europe. It was thus deduced that these spoofers were using this Middle Eastern operator as a transit point to 'filter' messages which would then be legitimately submitted to Western European operators, causing the Middle Eastern operator financial losses, as well as impacting the operator's roaming relations in carrying this spoofed traffic in the first place

MMS: the monitoring of MMS traffic revealed that over 15% of traffic exhibited illegal or undesirable content:

- Of this 15% a small percentage, (~2%), of MMS messages received contained illegal or undeliverable format. This meant that subscribers were being charged for MMS, which were not delivered. Using the NPP, this traffic was identified and blocked, thus preventing a financial impact to the subscriber, and subscriber care impacts to the operator.
- However the vast majority of this 15% contained different types of MMS viruses (see Figure 2), of which Beselo was the main variant. In this case the operator wished to remove the virus, but allow the message (as some messages may have been legitimately generated). Using the NPP's virus filters, the solution enabled modification of all message that were detected to have any type of MMS virus, before they are delivered to the recipient. This ensured that the spread of viruses was stopped.

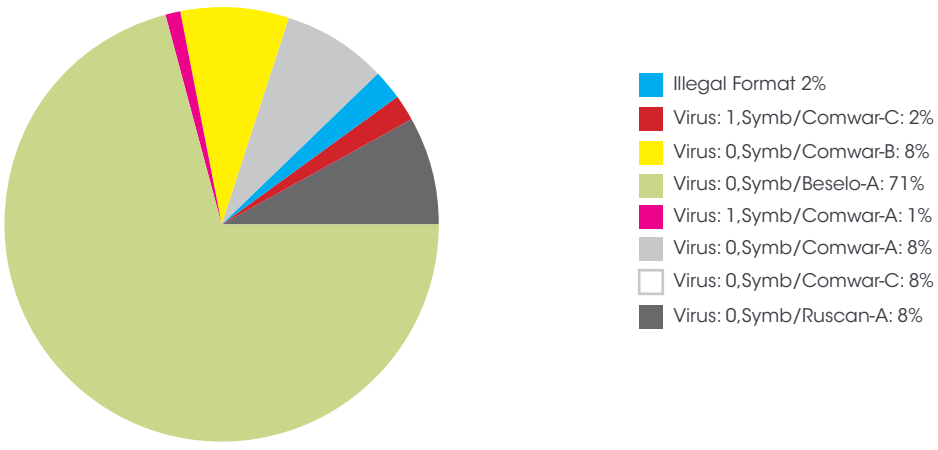

Figure 2: Distribution of MMS Viruses

Legitimate MMS were found to be infected with a variety of viruses - the Network Protection Platform is able to detect the infected messages, remove the virus and deliver them to their intended destination

[1]SymbOS.Hatihati.A is a Malware that sends a very high volume of SMS messages to a predefined number, mostly without the victim's knowledge, depleting the victim's airtime account.

[2]SMS Spoofing occurs when an SMS is sent with the senders address being impersonated a as if he/she roamed onto a foreign network and is submitting messages to the home network. Frequently, these messages are addressed to destinations outside the home network – with the home SMSC essentially being "hijacked" to send messages into other networks.

Outcome: Complete Security for the Subscriber

The deployment of AdaptiveMobile's NPP resulted in significant improvements for the operator and its subscribers. A summary of the benefits that were seen are:

• Viruses carrying messages (especially Hati Hati) that traversed the network have almost been eliminated.

• The elimination of SMS viruses, which was 20% of total SMS traffic and 15% of MMS traffic, resulted in a major reduction on the load on the operator's SMSC and MMSC. Thus the operator witnessed cost savings on SMSC and MMSC licensing.

• The operator witnessed less malware related traffic. This has had a positive impact on interconnect and roaming reconciliations, thereby limiting their losses.

• Using the Malware Recovery Module (MRM), the operator has been able to rollback the number of infected subscribers (i.e. using the AdaptiveMobile solution the operator has not only been able to stop the spread of viruses via messaging, but has reduced the number of infected devices that are present by removing the malware from them). This ability is crucial as there will always be methods of infection which do not involve the core network (such as Bluetooth, SIM cards etc), and thus the operator must strive to eliminate, not just prevent, infected traffic amongst the subscriber base.

AdaptiveMobile has earned the trust of the operator for its ability to handle network security challenges, both current and future. This has helped to deepen the relationship with the operator. It has also opened up expansion opportunities for the service to protect subscribers from additional forms of messaging fraud and abuse.

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

Head Office
Ferry House, 48-52 Lower Mount Street, Dublin 2.
Contact: sales@adaptivemobile.com

Regional Sales Contact Numbers:
US, Canada, Latin America Sales: +1 972 377 0014
UK Sales: +44 808 120 7638
Middle East Sales: +97144 33 75 83
Africa Sales: +27 83 7044111
Asia Sales: +66 89 87 42 32
European Sales: +353 (1) 524 9000

Regional Operational Support Contact Numbers:
UK: +44 208 114 9589
Ireland: +353 1 514 3945
France: +33 975 180 171
India: 000-800-100-7129
US, Canada, Latin America: +1 877 267 0444

For discussion of typical use cases, overview of AdaptiveMobile's existing deployments or a full walkthrough of service provider experience, contact your local office:

www.adaptivemobile.com/contact-us