M-Spam: From Network Protection to Revenue Assurance

April 2012

HAUD Systems - White Paper

Contents

M-Spam: From Network Protection to Revenue Assurance

If you had to simply do a quick search on the internet regarding SMS Spam or M-Spam, the amount of sites you would be directed to are just too many to mention. What does this tell us? It is indicative of the concerns that SMS spamming is ever increasing amongst mobile telephony users and their respective operators, alike.

- In the US for instance, from a survey carried out by Tatango it transpires that 68% of all Americans are effected by SMS spam[1].
- According to Whitepages.com, in the US, text message spam carrying malware links, which can damage your phone or steal personal information, has increased by 400% since the summer of 2010[2].
- In Pakistan, the PTA (national regulatory authority) has stated that 62% of Pakistani citizens use cell phones, especially for SMS. As a consequence, one can note an increase in marketing through SMS since it is considered a much cheaper, more personal and effective channel than other forms of marketing[3].
- In the UK, in December 2011, the Information Commissioner's Office stated that it carried out a survey of 1014 people of which 681 stated that had received a text that had caused them 'concern' and more than 200 said they were troubled by text spam[4].
- Moreover, the Australian regulatory authority said it saw a 370% increase in reports from the public about SMS messages believed to be spam between 2010 and 2011.

Despite the onset of internet on your mobile, smartphones and the upgrade of networks to UMTS technology and LTE, the large majority of handsets in the world are still regular mobile phones whose primary means of communication are still voice and text.

"...from a survey carried out by Tatango it transpires that 68% of all Americans are affected by SMS spam."

M-Spam vs E-mail Spam

M-Spam is a type of spamming, which has so far been directed at text messages on mobile phones themselves. With the onset of smartphones and data usage, this phenomenon is creeping over to data and its relative applications. Marketers are jumping onto the bandwagon of the M-Spam phenomenon as it is seen to be more personalised and instantaneous in comparison to email spamming.

Whilst email spamming requires the user to actually check his mail, mobile phones are carried around everywhere by their subscribers and SMS are checked instantly when received, unlike emails.

Despite email spam being combatted heavily over many years now and numerous anti-spam software being in existence to reduce the amount of spam reaching your inbox, these filters are not infallible and you will occasionally still receive email spam. The issue is exacerbated in the M-Spam scenario since unlike lessons learnt from its email legacy, spam filters on the mobile phone itself or on its operating system are not

a) easy to come by;

b) not as effective or as preventative in nature;

c) in cases where the called party pays principle applies, the user would still be charged for the SMS received despite this being filtered in the process (such as in the US).

"Marketers are jumping onto the bandwagon of the M-Spam phenomenon as it is seen to be more personalised and instantaneous in comparison to email spamming."

1 http://www.tatango.com/blog/text-message-spam-infographic
2 http://www.gottabemobile.com/2011/12/22/text-spam-costs-over-300-million-how-to-stop-call-and-sms-spammers-infographic
3 http://blogs.thenews.com.pk/blogs/2012/02/07/pta-needs-to-stop-sms-spamming
4 http://www.ico.gov.uk/news/current_topics/spam_text_survey_comments.aspx

Combatting M-Spam

To date the most 'effective' means to counter-measure M-Spam seems to be an open channel of communication whereby users and subscribers of mobile telephony operators are provided with a channel over which to submit complaints each and every time they receive such SMS spam to their mobile network operator.

In 2010, two major initiatives took place. The first is a GSMA pilot spam reporting program, and the development of Open Mobile Alliance (OMA) standards for mobile spam reporting. In its press release issued on the 24th March 2010 (London) the GSM Association stated that it was piloting a solution to address mobile messaging misuse caused by spam. Almost one year on, on the 10th of February 2011, GSMA went on to announce the findings from its pilot solution. During the pilot, SMS traffic was identified and analysed as well as aggregated reports of misuse, which consumers submitted via a short code to the networks participating in the said pilot. The conclusions were extremely interesting and insightful:

- spam is found across all networks;
- levels are higher than originally anticipated;
- addressing spam helps improve the security and stability of networks;
- lessens unwanted traffic on networks – freeing valuable bandwidth;
- most spam originates on-network, followed by peer networks and then through the Internet.

The GSMA Spam Reporting Services (SRS) highlighted three main categories of M-Spam, namely phishing attempts[5], social engineering scams[6] and premium rate fraud[7]. Some National Regulatory Authorities (NRAs) also refer to other scams such as mule spam[8] and Nigerian scams[9].

What is interesting to note is the regional differences in the types and message contents noted during the pilot. Asia predominantly focused on click fraud relating to gambling sites, followed by fraudulent loan services. Europe, on the other hand, had over 25% of reports relating to lottery fraud, followed by loan and insurance claim services. North America's reports related mainly to loans and payday advances.

In some countries, the introduction of limits on text messages being sent is used as a means to curtail spam. For instance, in June 2009, three major Chinese carriers, namely China Mobile, China Telecom and China Unicom, imposed limits on text messaging in order to crack down on spam SMS. Under the restrictions, a phone number can send no more than 200 messages per hour and 1000/day on weekdays.

In order to deter unsolicited text messages from being sent by telemarketing companies by millions daily, the Telecom Regulatory Authority of India (TRAI) has set a limit of 100 SMS per SIM per day to prevent fraudsters from spamming subscribers via SIM farms. In November 2011 however, it decided to relax this measure following representations received by some service providers and increased the statement to 200 SMS per SIM per day[10].

"The GSMA Spam Reporting Services (SRS) highlighted three main categories of M-Spam, namely phishing attempts, social engineering scams and premium rate fraud."

5 Phishing attempts are those situations where the spammer is attempting to collect financial information from the subscriber/user. These messages generally take the shape of content about some lottery win or a gift which one must claim by calling back or visiting a specific website.
6 Social engineering scams include loan or gambling scams where a subscriber/user is asked to reply to the sender and eventually convinced to transfer cash to the sender.
7 Premium rate fraud involves having a phone number embedded in the SMS content which the subscriber/user is solicited to call or text and then is charged at a premium rate for that number which premium rate charge is picked up by the attached.
8 Mule spam refers to criminals contacting prospective victims enticing them to divulge information through alleged job vacancy adverts.
9 Nigerian scams generally originate from alleged African countries (hence the name derivation) and usually offer to pay the recipient a sum of money if they assist in the transfer of millions of dollars out of the country of origin of the sender SMS.
10 http://www.trai.gov.in/WriteReadData/trai/upload/PressReleases/867/Press%20release%20for%20M2M.pdf

Top Text Message Spam Lawsuits

Burger King – $510,000 Lawsuit ($250/phone number)

A court approved a class action lawsuit settlement between lead plaintiff Elizabeth Espinal and Burger King over SMS SPAM. The Burger King SMS marketing class action lawsuit also names Textopoly, Inc. — the company that was hired to send the Burger King SMS campaigns and process the opt-out requests — as a defendant. Both companies deny any wrongdoing, but agreed to a $510,000 class action settlement to avoid on-going litigation.

Rolling Stones – $5 million Lawsuit

According to the complaint, Wenner Media and Consumer Benefit Services have been sending SMS Campaigns to cell phones of consumers offering vouchers for magazine subscriptions. The class action, led by an Indiana woman named Karen Schrock, claimed the SMS SPAM violated section 227 of the Telephone Consumer Protection Act, which restricts the use of automatic dialling systems to cell phones.

Timberland Company – $7 million Lawsuit ($150/phone number)

A settlement was reached with GSI Commerce, Inc. and The Timberland Company in a class action lawsuit relating to the alleged transmission of SMS SPAM to the cell phones of consumers nationwide. The $7 million dollar fund provided a $150 cash payment to each class member who filed a valid and timely claim. The settlement further provided a donation in the amount of $200,000 to a local charity.

Simon & Schuster – $10 million Lawsuit ($175/phone number)

In Satterfield v. Simon & Schuster, Inc., No. 07-16356 (9th Circuit June 19, 2009), the plaintiff sued the company (and its mobile ad agency) for sending text messages to her cell phone without the requisite permission. The district court dismissed her lawsuit; but in its ruling, the 9th Circuit revived it.

According to the lawsuit, some 60,000 cell phone users received SMS SPAM. Instead of going to trial and risking up to $90 million in damages, the defendants settled for $10 million.

Twentieth Century Fox – $16 million Lawsuit ($200/phone number)

A class action lawsuit settlement was reached with Twentieth Century Fox and FoxStore.com over sending SMS SPAM advertising the DVD release of the animated motion picture Robots. Twentieth Century Fox and FoxStore.com deny any wrongdoing, but have agreed to create a class action settlement fund of $16 million to settle the lawsuit. All class members were eligible to receive up to $200.

Nokia – 55,000 Australian Dollars ($57,750)[11]

The Australian Communications and Media Authority found that some of the texts Nokia sends to clients as tips to get more out of their phones promote Nokia without offering an “unsubscribe” option as required by local law.

The regulator said in a statement Nokia had agreed to train its employees engaged in SMS marketing about legal requirements and to pay a fine of 55,000 Australian dollars ($57,750).

11 http://www.acma.gov.au/WEB/STANDARD/pc=PC_410284

How Successful are Regulators in Attempting to Combat Spam?

USA

In 1991, the USA passed a federal law known as the Telephone Consumer Protection Act (TCPA). This limited the type of unsolicited calls, which could be made to landlines and wireless phones. The law was not that effective as the consumer was burdened to ask each telemarketer to put him/her on the do-not-call list. In 2003, the FCC introduced the Do-Not-Call Implementation Act which established the National Do Not Call Registry. These laws were further substantiated by the CAN-Spam Act which oddly enough does not provide adequate cover for text messages but is more focused on email messages, even if these are received on your wireless device. In fact the Act states that the FCC's ban covers messages sent to cell phones and pagers, (only) if the message uses an Internet address that includes an Internet domain name. However, despite these measures taken by the US authorities in order to curtail this phenomenon, around 68% of US mobile phone users are still affected by text message spam.

India

In India, in 2011 we saw the Telecom Regulatory Authority of India (TRAI) implement regulations forbidding telemarketers from sending promotional messages to subscribers on the Do-Not-Disturb Registry. The Authority attempts to clamp down on spam by sanctions such as the imposition of a Rs 25,000 fine for a first offender, which amount can increase up to Rs 2.5 lakh in a 6th offence as well as consequences of blacklisting – however these sanctions seem not to have had a significant impact on telemarketers. In fact only 3 weeks after the implementation of the regulation, commercial text messages had reverted back to their original numbers and expected to grow. Moreover, an increase in telemarketing calls was also noted.

Another aspect of the regulation actually caps the number of text messages on both prepaid and post-paid connections to 100 per day and 3,000 per month respectively. This has left some consumers in a country with over 700 million mobile phone subscribers, having to purchase more than one SIM card in order to be able to circumvent the restriction. So one wonders about the actual effectiveness for customers, since it certainly does not seem to have curtailed the illegitimate traffic but caused customers massive inconvenience in the process.

Australia

In Australia, ACMA (Australian Communications and Media Authority) enacted the Spam Act in 2003 which came into effect in April 2004. This law covers both commercial SMS and MMS, amongst other things. Despite the intention of the Act to curb unsolicited communication and encourage responsible marketing via SMS and MMS, when one looks at the ACMA website itself, one can see reports such as SMS Lottery Spam increased in October 2011, as well as a number of warnings having gone out through 2011 to various commercial entities for breaching the Spam Act.

''The Authority attempts to clamp down on spam by sanctions such as the imposition of a Rs 25,000 fine for a first offender...''

"...when one looks at the ACMA website itself one can see reports such as SMS Lottery Spam increased in October 2011..."

So What Now?

From the above, one can note that the primary focus and emphasis, both from large international associations like the GSMA with its SRS initiative, as well as NRAs, is on educating the consumer to protect itself and on clamping down on the actual perpetrators of unsolicited communications. However, from research and over 10 years of experience in the messaging industry, we have seen that:

a) consumers are not best placed to protect themselves from unwanted messaging;

b) marketers will always find a way to spam consumers, whether on a national level, through web2SMS applications, or via international routes;

c) NRAs and international bodies are well-meaning and their methods and activities are well-intended, however, not very effective in practice.

Our conviction is that prevention is the only way forward to combat M-Spam effectively and protect subscribers and the MNO. In order to guard consumers and clamp down on mobile spammers, the only effective solution is to implement a non-invasive, cost-effective, SMS filtering solution at the MNO level or as an outsourced or hosted solution in order to provide the benefit of statistical information about all traffic passing through the MNO network, a means of intervening on the traffic itself and ensuring that the MNO is capturing all revenue for such SMS traffic going through its network.

Let us just take a moment to look at the current typical mobile network being bombarded by M-Spam currently. Spam in this case may be coming from various sources such as local on-net marketers, off-net marketers within the same country or through third party bulk SMS providers who in turn sell traffic to the destination and the subscriber on that particular network. This can be done in many ways, and despite the fact that an MNO can try to curtail this activity by blocking certain Global Titles or Sender IDs from delivering traffic onto its network, it is a known fact that spammers have found ways for traffic to be re-routed and still reach its targeted mobile subscribers. What is more evident is that in view of volumes of SMS being transacted through bulk SMS providers, the price for SMS (be it national or international) is generally the subject of volume discounts and this means that it does not reflect the average market price for SMS or the established IOT in an AA.19 document for instance signed between two legitimate operators.

This, of course is still a best case scenario, where at least the MNO may charge for SMS terminated on its network, but there are also instances where SMS is spoofed or masked; in which case it is more difficult for operators to even detect such SMS or claim payment for the same being terminated on their network. Finally, there is also the customer side to the story were the customer is generally the victim of SMS scams, frauds and defamatory or scandalous content – which content is not filtered or blocked by the MNO. This creates a strained relationship between the MNO and its end-customer since customers complain about such messages to the MNOs call centre, customers may even decide to switch operator for such reasons and become generally unhappy with the service and lack of protection by the MNO.

On the other hand, if an MNO could pro-actively control its network and prevent the delivery of such M-Spam on its network, it could benefit in many ways by:

a) controlling the content of messages delivered on its network;

b) controlling which entities it allows to deliver such messages;

c) increase customer satisfaction, reduce call centre complaints and reduce churn;

d) charging proper market prices for SMS delivered to its network, despite the origination.

"...prevention is the only way forward to combat M-Spam effectively and protect subscribers and the MNO. In order to guard consumers and clamp down on mobile spammers, the only effective solution is to implement a non-invasive, cost-effective, SMS filtering solution at the MNO level..."

Conclusion

For all these reasons, HAUD Systems Limited has created a multi-layered protection system for MNOs through its scalable solution. HAUD Systems seeks to partner with MNOs and provide a comprehensive solution. The solution is based on various aspects from the offering of consultancy services to the MNO regarding the interpretation of the data on its network, which originators to block and how to ensure revenues are generated from all types of SMS entering the network. It also provides a non-intrusive software solution, which is flexible and upgradable instantaneously with new features offering the MNO peace of mind through the configuration of alarms, which the system pushes directly via email to the authorised personnel of the MNO. This solution need not necessarily be installed on the MNO's network itself, but can also be placed at SCCP carrier level for maximum protection and has the least invasive installation possible.

Finally, the most attractive feature of our offering is our commercial proposition to MNOs which effectively means zero capex and minimum opex to run.

If you would like to know more about HAUD Systems, please contact our sales team on sales@haudsystems.com or visit our website www.haudsystems.com.

Contact

For further information about HAUD Systems, please contact our sales team:

Email:	sales@haudsystems.com	Singapore:	+65 90 72 91 88
Malta:	+356 (0) 27 78 01 95	UK:	+44 (0) 203 411 0483
Sweden:	+46 (0)13 32 92 101	Americas:	+1 (212) 4191-320

HAUD Systems is a proprietary solution that is fully owned by 42 Group.

HAUD Systems