White Paper

The True Cost of SMS Spam

Prepared by

Patrick Donegan
Senior Analyst, *Heavy Reading*
www.heavyreading.com

on behalf of

CLOUDMARK™

www.cloudmark.com

May 2013

The True Cost of SMS Spam: A Case Study

With then-U.S. Secretary of Defense Leon Panetta warning last year of the risk of cyber-attacks that could "shock the nation" and the U.K.'s MI5 brought to its knees by super-smart, super-motivated cyber-terrorists in *Skyfall*, the latest James Bond movie, cyber security is moving front and center into our political and cultural landscape. Yet considered against the established fact of secret military data and billions of dollars' worth of Intellectual Property being stolen from government and businesses, and the very real fear of critical financial or energy infrastructures being disabled, the risk posed by a bit of SMS spam can appear a bit trivial.

The View From the CFO's Spreadsheet

But look at it from the day-to-day perspective of a mobile operator and its responsibilities to customers, employees and shareholders, and actually SMS spam isn't at all trivial. On the contrary, SMS spam is generating significant recurring costs for many mobile operators, with dismal predictability from one financial quarter to the next. As we demonstrate in this paper, if SMS spam is left unaddressed, a mobile operator with 10 million subscribers can easily incur an annual cost of almost $6 million just in call center costs and asymmetrical inter-operator SMS termination charges. Since there are proven SMS filtering solutions readily available on the market that can eliminate the bulk of these costs from the CFO's spreadsheet, the only reason the problem continues on its current scale is the relatively low profile it has had until recently.

The immediate, demonstrable near-term costs of SMS spam aren't the only issue either. Those mobile operators that are at the very cutting edge of the mobile broadband applications and service revolution recognize that security vulnerabilities in any part of the ecosystem undermine their prospects of monetizing the next big market opportunities. In May 2012, for example, Randall Stephenson, Chairman, CEO & President of AT&T, told an audience at The Milken Institute that "the long pole in the tent" when it comes to capturing the new revenue opportunities in areas such as mCommerce and mHealth "is going to be getting the ecosystem to be robust in protecting data and making sure you control who sees the data, how it's shared and how it's transmitted. Until you get it right, there is going to be inherent apprehension and concern by all of us about this."

More Volume, More Diversity

For the purposes of this white paper, the term "SMS spam" is used as an umbrella term within which is included the following:

- Unsolicited bulk marketing, advertising or solicitations, fraudulent offers and "phishing" messages.
- Viral messages having no purpose other than to generate vast volumes of SMS traffic, running into the many millions.
- Messages that invite the user to reply by text or call a premium-rate number, either of which generates a high charge on their bill.
- Social engineering messages that contain embedded links to malware such as Trojans that automatically send premium-rate SMS messages without the user's knowledge or form part of a coordinated attack combining SMS with other attack vectors, such as email, voicemail or rogue links to websites.

14 Trillion SMS Messages per Year

According to the ITU the number of SMS messages sent worldwide increased from 1.8 trillion in 2007 to 6.1 trillion in 2010. *Heavy Reading* estimates the number could exceed 14 trillion in 2013 – representing about 2,000 SMS messages per person on the planet. Over-the-top (OTT) messaging applications will certainly provide strong competition to SMS, but all this will do is slow the rate of SMS growth at some point in the future. Most countries are many years away from seeing annual growth in SMS traffic begin to flatten out, let alone seeing total SMS traffic go into decline.

Even if only 1.5 percent of the more than 14 trillion SMS messages expected this year are spam, that is more than 200 billion spam messages that will be sent this year. And while 1.5 percent might be a common ratio in developed markets currently, it can be higher in some developing countries, even reaching as high as 30 percent. And if 1.5 percent doesn't sound like much, consider nevertheless that both Cloudmark and Kaspersky Labs are among the leading mobile security vendors that have demonstrated in the last 12 months that more than 50 percent of malware detected on smartphones currently consists of SMS Trojans.

Even if the proportion of SMS traffic that is spam remains constant, total SMS spam volumes will continue to rise in line with total SMS traffic. Industry trends don't point to SMS attacks becoming any less attractive to attackers. Quite the contrary: Many industry trends are increasingly favorable to SMS spammers.

Industry Trends Make SMS an Increasingly Attractive Attack Vector

1. **Smartphones and tablets are rapidly replacing fixed phones and PCs for an increasing proportion of communication needs.**

Due to their ever-increasing processing power, the personal data they store, how trusted they typically are by users compared with PCs and the impulsive behavior they encourage, smartphones and tablets provide attackers with a platform that is uniquely vulnerable to sophisticated cyber-attacks across the media of telephony, email, IM, SMS and MMS.

2. **Further declines in SMS pricing, including unlimited SMS bundles, have the effect of lowering the cost to attackers of sending SMS messages in bulk.**

The rate of SMS price decline is driven by local competition between operators and increasingly by the rise of OTT messaging applications.

3. **Application-to-person (A2P) bulk messaging, whereby businesses and other organizations harness the power of SMS for mass-marketing efforts, is continuing its growth.**

The way "SIM boxes" avoid international call charges by making off-net international calls appear as on-net calls is well known. What is less well known is how widely these devices have been repurposed to generate huge volumes of SMS messages at negligible cost to the spammer. There is innovation at the low end of the volume message-generation market, as well. For example, the "Kickstarter" website, which crowd-sources high-tech venture funding via online micro-payments, recently funded the so-called SMuShBox. This device promises to enable super-low-cost mass-market texting for small businesses by "cutting out the middlemen and monopoly of the Common Short Code Administration (CSCA)," which upholds the operator's revenue share in A2P bulk messaging.

4. **One specific feature of the smartphone, derived from its processing power and the increasing bandwidth of mobile networks, is its ability to serve as a bot in a botnet, and therefore serve in a mobile botnet for churning out SMS spam.**

Mobile botnets have been anticipated for some time, but they are now a reality. In December 2012, for example, Cloudmark discovered the "SpamSolider" Android botnet, designed to leverage Android devices to send malicious SMS spam under the direction of a controller using HTTP GET requests. The botnet's command and control server was taken down within a few days of the spamming activity being discovered, but not before between 5 and 10 million SMS messages had been sent, and between 1,000 and 2,000 Android smartphones had been infected. Mobile botnets are fact now, not fiction.

More Sophistication, Nastier Impacts

SMS spam is following the curve of email spam with respect to the sophistication of attacks that we are seeing now. The simple, clumsy, "Who on earth would fall for that?" type of email from an "heiress" promising a substantial cut of her "$15 million inheritance" has roots in another era. Today attackers aren't prepared to waste time hoping that you'll be fooled into wiring them money. At the nastiest end of the spectrum, SMS attackers are out to steal money from subscribers without them even knowing about it.

The majority of spam might appear to be less nasty than this, but as is the way with messaging attacks, even this appearance is deceptive. Take, for example, the increasingly common SMS invite to enter a competition and win a free iPad – an attack that has become increasingly common in the last 12 months. In many markets, either a majority or a substantial minority of consumers are prone to believing that their chances of winning the iPad via this "invitation" are remote, when in reality their chances are nearly always nonexistent.

Moreover, consumers often have little or no understanding that scammers can make money from selling on their personal information – their name, age, address, income, employment status, etc. – to third-party marketing organizations. They also have little or no understanding of the long-term damage that can be done to them by the disclosure of their personal information on the open Internet (for example, with respect to impacting their applications for credit or health insurance). And they have little or no knowledge that the terms and conditions of the "free" competition for an iPad sometimes contains a clause in the fine print authorizing a few dollars to be debited from their mobile phone bill.

According to *Heavy Reading*'s 2012 mobile operator survey on mobile network security, the vast majority of mobile operator respondents recognize that some of their subscribers have already fallen victim to theft via some kind of attack by a hacker or spammer.

New Attacks Appear Increasingly Plausible to Consumers

SMS attackers these days are increasingly sophisticated and able to craft and time their attacks to exploit the unique realities – usually the unique economic realities – of the local market. For example, Cloudmark's 2012 Messaging Threat Report identifies surges in tax-related SMS scams in the run-up to government deadlines for submitting tax returns.

The report also identifies surges in SMS attacks inviting users to appeal for compensation timed to coincide with legal rulings against companies deemed to have broken the law with respect to their treatment of consumers. And it identifies peaks and slumps in the volumes of SMS attacks relating to rogue payday loans that map very closely to the ups and downs in unemployment benefit claimants in the local market. According to Cloudmark, there were 30,000 unique SMS spam pitches per month to mobile phone subscribers throughout 2012, or a total of approximately 359,000 unique pitches throughout the year.

As already alluded to, attackers are also using greater and greater sophistication in the form of leveraging multiple communication paths or protocols across the mobile network, fixed network and social networking domains to sharpen the believability of SMS spam and generate impacts that are a lot more successful for the attacker, hence a lot nastier for the user.

One of the first was the Zitmo Trojan back in 2010, which blends conventional Internet attack methods to steal a user's banking credentials and mobile phone number from their PC with a second-phase attack, in which an embedded link in a bogus SMS message causes the user to inadvertently authenticate a transaction from their own bank account.

In the last year, we have seen more such blended attack types. Some attacks combine SMS with recorded messages on voicemails that exactly mimic the pre-recorded voice messages used by leading banks. These days, three-stage attacks are also increasingly common – for example, attacks that start with an SMS message, then move to an IM platform, before executing the final stage of the attack on a website.

Escalating Costs to the Mobile Operator

Dealing with the symptoms of SMS spam once the mobile operator has allowed it to enter the network and reach subscribers is generating a substantial cost burden. The costs can be broken down into different components, some of which are obvious and well understood, but some of which are not. These include:

- **Unnecessary SMS Termination Charges.** With SMS in most countries, the "calling party pays" principle applies to the operator just as it does to the end user. In other words, the operators pay for each and every message that they send one another – irrespective of whether those messages are legitimate or not. So if Operator A and Operator B each have 10 million customers and send one another 1 billion SMSs per month, of which 18 million from Operator A are spam but only 8 million from Operator B are spam, then Operator A is sending – and therefore paying for – 10 million more spam messages than Operator B. Assuming a typical SMS termination rate of 0.03 cents per message, then as a result of this asymmetry Operator A is directly paying Operator B $300,000 every month or $3.6 million per year for these additional spam messages.
- **Calls to Customer Care Centers:** A customer that thinks he has been the victim of a scam is quite likely to tie up call center resources with a complaint or an enquiry. For example, an operator with 10 million customers need only have 0.75 percent of its customers contact its call center twice per year about SMS spam – at a cost to the operator of, say, $15 per call – and that constitutes an annual cost there of $2.2 million.

- **Excess Capex.** In a minority of cases where spam starts to comprise much more than 20 percent of total SMS traffic, then operators also need to factor in the cost of supporting that in terms of the capital that is needlessly spent on its SMS infrastructure that are tied up in supporting this traffic.
- **Foregone Revenues.** Leveraging their trusted brands to offer customers a chance to compete for an expensive holiday, a car or a season ticket to their favorite sports team via a text costing a dollar or two has potential to be a very attractive business model for mobile operators. But if that trust is corrupted by spam that promises the same prizes – but never delivers them to anyone – the operator will not be able to maximize that revenue opportunity and may even have to forgo running such competitions altogether in order to protect their brand.

As the sheer volume and sophistication of SMS attacks increases, it follows that if steps aren't taken to address the problem, then the cost burden must inevitably increase as well.

Spam Filtering: There Is No Alternative

This paper has demonstrated that there is a significant cost to the operator associated with SMS spam. Then again, the kind of high-end message filtering solutions that can take more than 95 percent of the malicious SMS and other abusive messaging out of your network altogether and ensure it never reaches your subscribers doesn't get given away for free.

High-end message filtering solutions cost money. They also require management attention. So what arguments are there for leaving this problem to loiter somewhere in the bottom half of the operator's "to do" list, while new subscriber acquisition, network build-out, new value-added services and new ARPU generators continue to preoccupy the business? Below, we consider four of the most common arguments for delaying the introduction of high-end message filtering solutions, or declining to invest in them at all.

1. **"The other operators in our market suffer from SMS spam just as we do. It's a level playing field, just a cost of doing business."**

This just isn't true. As has been demonstrated, each operator has its own unique profile of incoming and outgoing SMS spam. It also has its own its own unique profile of direct and indirect costs, its own unique profile of dissatisfaction caused to subscribers, and its own unique reputation among consumers, regulators and other operators. Available evidence also points to large fluctuations in SMS spam origination according to the steps that different operators take to deal with it. For example, when one operator introduces solutions to prevent outbound spam from leaving its network, large volumes of spammers tend to move very quickly to another operator in the market, where they can expect a better success rate.

2. **"SMS tariff rebalancing is a lower-cost way of addressing the problem."**

Low pricing of SMS, especially large bundles and unlimited offers, is certainly a part of the problem, in that it lowers the cost of doing business to spammers. Far too many operators continue to make short-sighted, inappropriate, ARPU calculations from acquiring low-end subscribers with cheap SMS bundles. They continue to fail to factor in the real costs that some of these new subscribers will undoubtedly generate with their abuse of the operator's messaging platform.

In theory, operators can restrict the number of texts that any one subscriber is allowed to send. They can raise the price of texts, especially large and unlimited bundles. And they can single out pre-paid packages, whose users are harder to trace than post-paid users, for tighter restrictions. But while some of these measures might have an effect of some kind at the margin of the problem, many of them fly in the face of the commercial realities of day-to-day price competition.

Lastly, consider how adept attackers are at adapting to and getting around such barriers that focus on pricing. In practice, for example, a smart operator dare not just automatically cut off a user after they have exceeded a limit on sending SMS, because that subscriber's smartphone may have innocently become part of a mobile botnet. That operator needs to focus on detecting the botnet's behavior, rather than just that of the individual subscriber.

3. **"Our government relations people are working with regulators, lawmakers and law enforcement to address the problem at its source by arresting, charging and punishing SMS spammers."**

It is certainly true that regulators in leading markets are starting to get involved. In March 2013, for example, the Federal Trade Commission filed eight complaints in U.S. courts against 29 defendants for allegedly sending more than 180 million spam SMS messages. But this process is still in its early stages in most countries and hasn't gotten underway at all in many countries.

Moreover, even once law enforcement does engage, only some perpetrators will be caught, only some of those will be punished, and only some of those will be punished effectively. Just because we have a police force doesn't mean we don't lock our front doors at night; likewise, just because the law engages in the battle against spam doesn't make investment in other defenses unnecessary or superfluous. Also consider how many years regulators have been trying to combat email spam, with little to show for it – in part because it only takes a few rogue countries to turn a blind eye to the problem, and spammers in those countries can remain free to act with impunity, impacting operators all over the world.

Moreover, the engagement of regulators is also a double-edged sword for mobile operators. Some regulators won't just look to fine and otherwise punish spammers; they will also target those operators that don't take the necessary steps to protect consumers. For example, Chile's consumer protection agency recently filed a legal complaint against mobile operators Claro, Movistar and Entel, for allegedly not allowing Chilean consumers to block bulk promotional SMSs.

And the last thing any mobile operator CTO wants is a regulator that identifies a vacuum where a technical, network-level fix for the problem ought to be. That regulator is then liable to make it its mission in life to draw up its own technical, network-level fix and mandate that every operator in its market has to implement it, rather like the Telecom Regulatory Authority of India (TRAI) has done.

4. **"It is better to allow a hundred spam messages get to your subscribers than to have a security solution mistakenly delete one legitimate one."**

The generation of so-called false positives – flagging or acting on legitimate traffic in the belief that it may be abusive – is certainly a common cause of dissatisfaction among network security professionals with any network security product. But in the case of messaging security solutions, there are leading products out there that can deliver a very low rate of false positives. Moreover, consumer attitudes to email spam show that the large majority are prepared to tolerate the occasional

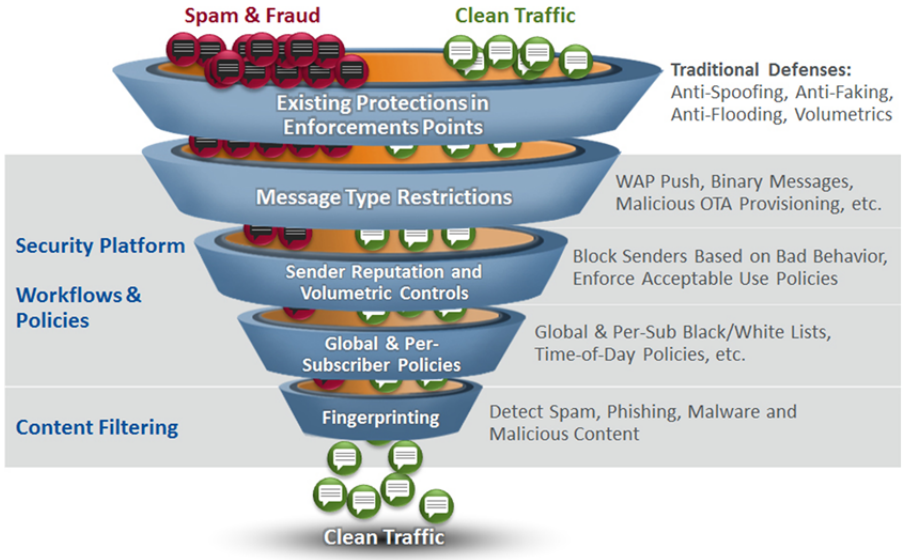
false positive in exchange for stemming the deluge of incoming abusive email before it hits their inbox. As SMS spam volumes increase, there is every reason to think that the consumer perspective on SMS filtering will go in the same direction.

Key Requirements for Spam-Handling

This paper has identified SMS spam as generating a variety of direct and indirect costs for the mobile operator. It has demonstrated that each operator's profile of costs incurred is a unique reflection of its positioning in the market with respect to the variety of steps it takes – or doesn't take – to address the problem.

Messaging filtering and protection solutions are a critical component of the mobile operator's stance against the costs of SMS spam. They provide the key tools with which the operator can reduce its costs by blocking outgoing abusive messages from its own rogue subscribers, as well as inbound abusive messages that are targeting its entire subscriber base.

Figure 1: Key Requirements for Spam-Handling



Source: Cloudmark

High-end messaging security solutions share a number of key characteristics. They need to be software-centric and evolvable to rapidly respond to the highly dynamic behavior profile of spammers. Real-time message scanning will inevitably deliver the best results – so long as it introduces only minimal latency. Their attack techniques and tactics change very rapidly, so any messaging security solution needs to be able to evolve in step with changes in those techniques and tactics.

The solution needs to have access to a leading Global Threat Network, since threats can emerge from anywhere and do not respect geographical boundaries. And a high-end messaging security solution also needs to be cross-platform – detecting threats that emerge first in email or the social networking environment and move over into the SMS space, or reuse the same URLs, etc.

Background to This Paper

About Cloudmark

Cloudmark (www.cloudmark.com) builds messaging security software that protects communications service provider networks and their subscribers against the widest range of messaging threats. Only Cloudmark Security Platform delivers instant security and control across diverse messaging environments, enabling communications service providers to create a safe user experience, protect revenue and safeguard their brand, while streamlining infrastructure and reducing operational costs. Cloudmark's patented solutions protect more than 120 Tier 1 customers worldwide, including AT&T, Verizon, Swisscom, Comcast, Cox and NTT.