CLOUDMARK®

Taxonomy of Current and Potential Mobile Threats

Christopher Abad, Research Scientist

INTRODUCTION

The users of traditional messaging services are well aware of the forms of abuse they face on a regular basis. Spam, phishing and viruses found in email are so common that these terms are part of our collective lexicon and need no definition. Emerging classes of messaging abuse in the mobile environment, however, have led to neologisms like “smishing,” or SMS phishing. Are these mobile threats real, or are they simply media-constructed FUD (fear, uncertainty, doubt) that ultimately distracts security managers from more imminent and damaging threats?

This paper provides a broad consideration of all potential messaging threats that may confront wireless operators and breaks them down into two broad categories: (1) wireline-to-wireless threats and (2) wireless-specific threats. These two threat types are considered individually due to technical and economic reasons, which play key roles in how likely they are to proliferate in the wireless environment and what are the appropriate methods to stop them.

WIRELINE-TO-WIRELESS THREATS

Technology convergence has helped decrease the cost of devices and services that bridge traditional wireline services such as email and Web and wireless services such as SMS and WAP. Economic barriers, such as the relatively high cost of sending SMS from a handset, have kept the wireless space almost clear of the volume of messaging abuse seen by wireline networks. This barrier, however, has been lowered by the increasingly seamless interface between the two technologies. Email to SMS gateways enable any email user to send messages free of charge to mobile subscribers around the world. Since spammers are not penalized for sending SMS/text messages, this potentially opens up the possibility of low-profitability spam, like the “Viagra” spam, being an issue for mobile users.

Email to SMS is a popular service that subscribers use to reach friends and page groups of users, so discontinuing or severely restricting this service is not a good option. Therefore, mobile operators need to protect their email to SMS gateways with the same type of filters and content analysis systems that large ISPs use to cover their email infrastructure. As mobile customers demand more features currently available only over the Internet, the economic constraints that restrict mobile messaging abuse will disappear, leaving mobile devices vulnerable to the same forms of messaging abuse as those terminating on laptops and computers.

To make matters more complicated, email and other forms of communications are extending to new categories of devices beyond just mobile phones and PDAs. Internet connected devices ranging from television set-top boxes to refrigerators are rapidly expanding the footprint of messaging-capable platforms. The latest wave of gaming consoles and portable entertainment devices also have Internet connectivity and messaging capabilities, which raises additional concerns about inappropriate content reaching minors who are the majority of users of these devices. While the incidence of abuse on these platforms is still unknown, the sheer number of these devices together with the affinity of the users makes these platforms compelling targets for spammers.

WIRELESS-SPECIFIC THREATS

Wireless-specific messaging threats will be similar to those pioneered in the wireline domain, but will diverge due to specific economic factors. Asia has consistently led the way in mobile content and usage trends, and events there may be indicative of what’s to come in other developed mobile markets such as the U.S. and Europe. In Japan and South Korea, where the cost of sending SMS is around a penny, the rate of mobile spam is almost on par with email spam. On Japan’s NTT DoCo-

Mo's network, 9 out of 10 messages are spam. In South Korea, subscribers receive on average one spam per day on their mobile phone.

Until the per message cost associated with sending SMS drops in the U.S. and Europe, users there will likely see short codes and narrowly-targeted announcements instead of URLs and large broadcast mailings that are prevalent in wireline networks. For example, a user may receive a spam SMS enticing him to sign up for a text service using a short code that is tied in with the mobile operator's billing system or he may be tricked into calling a premium rate number. The ease in setting up premium rate phone numbers makes this type of fraud particularly appealing to scam artists. These "false pretext" messages have a direct and immediate monetary impact on subscribers, leading to high customer dissatisfaction.

"Smishing" Attacks

Mobile banking and mobile payment have proven to be hugely popular in Japan and South Korea, with tens of millions of subscribers participating. The shift from bank tellers to mobile phone is occurring since it is increasingly being recognized by banks as a cost-effective way to deliver banking services. Financial institutions around the world are offering SMS services such as account access via SMS and SMS alerts that inform customers of account activities that have taken place such as transactions or overdrafts.

Economic incentives for phishers, previously missing in the mobile environment, now exist. This new direct interaction between the bank and the mobile consumer creates an opportunity for phishers to gather financial information from mobile users for identity theft and other types of fraud. Some of these attacks ask recipients to register for a service – after which they attempt to get users to accept a virus on their handset or to extract credit card numbers and other private data. Anecdotal reports of SMS phishing against users of pre-paid mobile phones have also surfaced, where recipients are asked to enter their account information to recharge their cell phone minutes.

Large-scale SMS phishing or "smishing" probably will not occur until shortly after most major banks offer these services and a sufficient number of users have adopted. In the interim, these attacks will occur sporadically. The reduced volume of attacks require solutions that do not depend upon volume-based content blocking but, instead, can rapidly react to both user feedback and preemptively stop attacks detected via honeypots and other sensor networks.

Mobile Viruses and Worms

The emergence of wireless malware as a widespread problem depends upon the standardization of mobile software and platforms. A critical mass of homogeneous software is not yet available for self-propagating malware to establish itself in the mobile community. This situation has been demonstrated by the large
number of Symbian OS variants that, while making news in the anti-virus community, have not actually impacted many users. As the popularity of mobile devices with operating systems such as Windows Mobile or Symbian increases, the likelihood of mobile viruses occurring will also rise.

THE IMPACT OF UNCHECKED MOBILE MESSAGING ABUSE

While spam is annoying to users on email, it is intrusive and costly on mobile devices. An SMS message can interrupt the subscriber at anytime, and in the U.S., these unwanted interruptions usually have a hard cost per message. Moreover, fraudulent messages inviting calls and messages to premium rate numbers can have a monetary impact many times greater than the usual SMS send/

receive costs. Therefore, mobile spam is more likely to trigger calls to customer support to register complaints or to ask for credits.

Mobile phishing has even more serious financial and privacy implications for the subscriber, which. jeopardizes the relationship between the subscriber and the financial institution. Mobile spam can also break the bond of trust between the subscriber and the service provider. This lost trust will make it difficult for subscribers to accept legitimate mobile advertising from the operator and its partners.

Finally, an unchecked flood of SMS spam can have serious ramifications on the mobile operator's quality of service. SMS messages are transmitted over the same channel as voice calls, so a large volume of SMS spam is capable of overloading the network and leading to denial of voice services. While some next generation SMSCs have the capabilities to rate-limit the traffic sent over the SMS network, it is often not the case with legacy installed equipment. Additionally, there are usually very few controls on the rate of reception of traffic from external networks, since externally originated MT SMS traffic is sent directly to subscriber MSCs

MECHANISMS FOR CONTROL

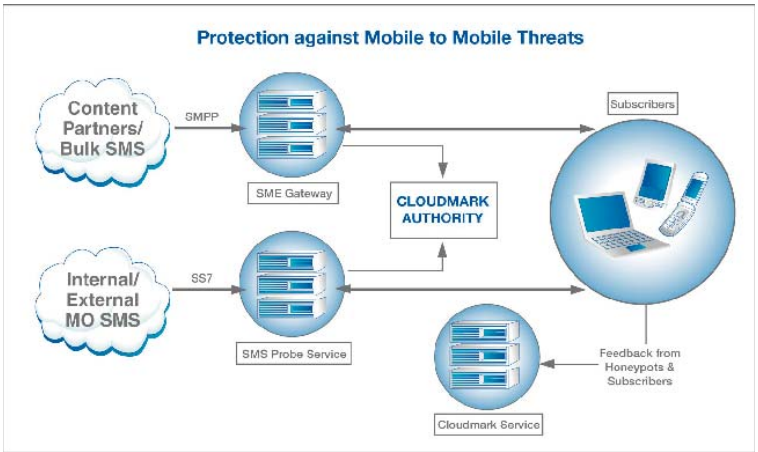
Even though text-based spam is on the rise, the number of spam messages that actually get through to subscribers is relatively small compared to the overall volume of mobile messages sent world-wide.

Why is mobile messaging abuse still emerging? Mobile operators have several means to control spam originating within their own network, including blacklisting the message center, barring the number from sending to their network, or blocking the subscriber from sending. Spam originating from overseas networks or that come from the Internet, however, is more difficult to control. Spam originating from overseas networks requires cooperation from other service providers, while spam coming from the Internet requires third-party filtering solutions that can implemented at the MTAs or the email-to-SMS gateways.

Cloudmark's content-agnostic messaging anti-abuse solutions are uniquely able to combat mobile spam, phishing and viruses. While other solutions rely on memory-intensive rules or statistical analysis, Cloudmark Authority uses continuously updated feedback from its Global Threat Network to determine which messages are spam and which are legitimate. Traditional solutions employing heuristics often cannot distinguish spam from legitimate text messages. Cloudmark's approach is to integrate the Authority engine at key places in the network infrastructure to prevent messaging abuse from being received into the carrier network.

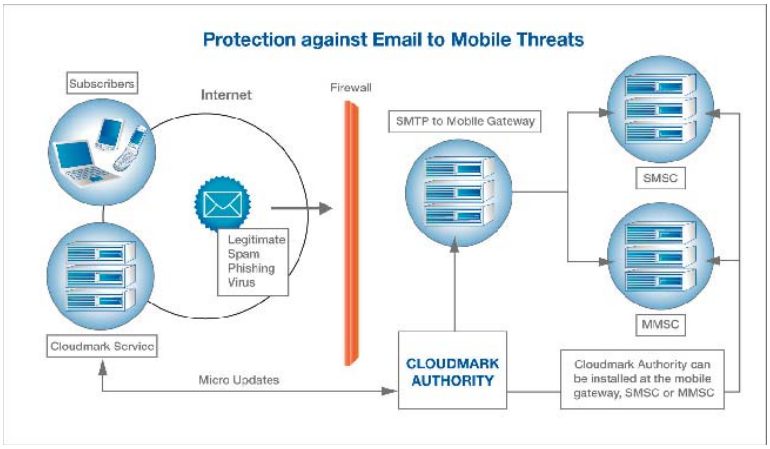
Cloudmark Defense against Mobile Originated Threats

For combating mobile to mobile threats originating from internal sources or external networks, Cloudmark has partnered with mobile messaging platform providers such as Anam (www.anam.com). The Anam-Cloudmark solution for countering SMS spam integrates a patent-pending SMS probe service, which is capable of intercepting traffic in real time and then filtering it using the Cloudmark Authority engine. This solution has the unique ability to trap messages to honeypot accounts and then forward them to the Cloudmark Global Threat Network to provide near real-time protection against new types of threat. Cloudmark Authority can also be integrated into the SME gateways used to accept traffic from content partners and bulk SMS senders.



Cloudmark Defense against Wireline Originated Threats

To stop messaging abuse originating from the Internet, including email and MMS, Cloudmark Authority is integrated with edge MTAs and MMSCs. As in the case with handling wireless threats, Cloudmark offers rapid response to new attack vectors through the Cloudmark Global Threat Network consisting of feedback from service providers, subscribers and honeypots.



CONCLUSION

Future price reductions on messaging anticipated in the U.S. and Europe will encourage mobile marketing and greater usage of SMS services. However, it may also invite new classes of wireless-originated abuse as seen in the Japanese and South Korean markets. With the potential for spammers and phishers to tap into the wallets of mobile users, it's only a matter of time before mobile operators experience a surge of messaging abuse (which continues to grow steadily in the wireline environment).

Mobile spam and phishing can kill the adoption of nascent services such as mobile banking services and mobile marketing. For example, predicted revenue growth for mobile advertising in Europe could be severely derailed by a proliferation in the types and volume of mobile abuse. Rather than wait for mobile messaging abuse to be epidemic, mobile operators should take steps now to proactively protect themselves and their subscribers against mobile- and Internet-originated threats.

Cloudmark's flexible, content-agnostic solution is uniquely able to combat mobile spam, phishing and viruses that originate from mobile devices or the Internet. By leveraging continuously updated message fingerprints along with feedback from the Global Threat Network, Cloudmark Authority is able to accurately block mobile threats while ensuring legitimate messages reach subscribers without interruptions. Cloudmark can be implemented to stop messaging abuse at the network's edge, thus ensuring that spectrum, network resources and service quality are not impacted. For mobile operators, Cloudmark's comprehensive messaging security leadership translates into lower subscriber churn and support, as well as loyal subscribers who can confidently adopt innovative services.

For more information
visit us at www.cloudmark.com

Americas Headquarters
Cloudmark, Inc.
San Francisco, USA

Asia Pacific Headquarters
Cloudmark, Inc.
Singapore

Europe Headquarters
Cloudmark Europe Ltd.
London, UK